Journal of Computer Applications
计算机应用,2013,33(11):3244-3246,3266
ISSN 1001-9081
CODEN JYIIDU
2013-11-01
http://www.joca.cn

文章编号:1001-9081(2013)11-3244-03
doi:10.11772/j.issn.1001-9081.2013.11.3244

关于 RSA 算法中代数结构的进一步研究

裴东林*,李 旭
(兰州文理学院 师范学院,兰州 730000)
(*通信作者电子邮箱 pdksxpdl@163.com)

摘 要:针对 RSA 算法中$\mathbf{Z}_{\varphi(n)}^*$的代数结构问题,提出了一种在强素数条件下应用二次剩余理论进行研究的方法。给出了$\mathbf{Z}_{\varphi(n)}^*$中元素阶的计算公式和元素的最大阶表达式,计算了$\mathbf{Z}_{\varphi(n)}^*$中二次剩余的个数和二次非剩余的个数,同时估计出$\mathbf{Z}_{\varphi(n)}^*$中元素的最大阶上限为$\varphi(\varphi(n))/4$并得到了$\mathbf{Z}_{\varphi(n)}^*$中元素的最大阶达到$\varphi(\varphi(n))/4$的一个充要条件。另外还给出了全部二次剩余构成的子群A_1成为循环子群的充分条件及$\mathbf{Z}_{\varphi(n)}^*$的一种分解方法。最后证明了$\mathbf{Z}_{\varphi(n)}^*$可由 7 个二次非剩余元素生成,商群$\mathbf{Z}_{\varphi(n)}^*/A_1$是一个 Klein 八元群。

关键词:RSA 算法;代数结构;二次剩余;强素数;循环群;欧拉函数
中图分类号:TP301.6 **文献标志码**:A

Further study on algebraic structure of RSA algorithm

PEI Donglin*, LI Xu
(*Normal College, Lanzhou University of Arts and Science, Lanzhou Gansu 730000, China*)

Abstract: By making use of the theory of quadratic residues under the condition of strong prime, a method for studying the algebraic structure of $\mathbf{Z}_{\varphi(n)}^*$ of RSA (Rivest-Shamir-Adleman) algorithm was established in this work. A formula to determine the order of element in $\mathbf{Z}_{\varphi(n)}^*$ and an expression of maximal order were proposed; in addition, the numbers of quadratic residues and non-residues in the group $\mathbf{Z}_{\varphi(n)}^*$ were calculated. This work gave an estimate that the upper bound of maximal order was $\varphi(\varphi(n))/4$ and obtained a necessary and sufficient condition on maximal order being equal to $\varphi(\varphi(n))/4$. Furthermore, a sufficient condition for A_1 being cyclic group was presented, where A_1 was a subgroup composed of all quadratic residues in $\mathbf{Z}_{\varphi(n)}^*$, and a method of the decomposition of $\mathbf{Z}_{\varphi(n)}^*$ was also established. Finally, it was proved that the group $\mathbf{Z}_{\varphi(n)}^*$ could be generated by seven elements of quadratic non-residues and the quotient group $\mathbf{Z}_{\varphi(n)}^*/A_1$ was a Klein group of order 8.

Key words: Rivest-Shamir-Adleman (RSA) algorithm; algebra structure; quadratic residue; strong primer; cyclic group; Euler's Phi-function

0 引言

1978 年,三位数学家 R L Rivest, A Shamir 和 L Adleman 提出了一种基于大整数分解困难问题的密码算法,称为 RSA 算法[1],众所周知,RSA 算法是目前最能被人们接受也是最被广泛使用的密码算法之一。对 RSA 算法及其安全性研究一直是数学界、密码学界关注的热点问题。RSA 算法的安全性基于大整数分解问题的困难性,针对"大整数分解问题",最好的攻击算法是数域筛法[2],除此之外,还有许多 RSA 算法及其安全性的研究成果[3-5]。另一方面,文献[6-7]从代数结构的角度对 RSA 算法中$\mathbf{Z}_n^*$及$\mathbf{Z}_{\varphi(n)}^*$的代数结构进行了研究并取得了一些成果。本文在强素数条件下,对 RSA 算法中$\mathbf{Z}_{\varphi(n)}^*$的代数结构作了进一步研究,得到了一些新的结果,这对于从代数结构的角度分析 RSA 的安全性有着重要的意义。

本文记号的规定:$\mathbf{Z}_{\varphi(n)}$表示模$\varphi(n)$下的剩余类,$\mathbf{Z}_{\varphi(n)}^*$表示模$\varphi(n)$下且与$\varphi(n)$互素的剩余类,$\varphi(\cdot)$表示欧拉函数,$\gcd(x,y)$表示$x,y$的最大公约数,$\mathrm{lcm}(u,v)$表示$u,v$的最小公倍数,$<a>$表示由元素$a$生成的循环群,$|b|$表示元素$b$的阶,$|A|$表示集合$A$中元素的个数,$xA$表示元素$x$与集合$A$中每个元素左乘所得的集合。当$m$为素数时,符号$\left(\frac{a}{m}\right)$表示$a$对$m$的勒让德符号。

1 RSA 密码体制

RSA 算法的基本思想是:首先选取两个大素数p,q;然后算出$n=pq,\varphi(n)=(p-1)(q-1)$再选取正整数$e$,使得满足$1<e<\varphi(n),\gcd(e,\varphi(n))=1$;再选取正整数$d$,使之满足$1<d<\varphi(n),ed\equiv 1(\mathrm{mod}\ \varphi(n))$。用$(e,n)$作为公钥,用$(d,p,q)$作为私钥。

加密算法 任取消息$m\in\mathbf{Z}_n$(必要时可对消息进行分块),计算出密文$y=m^e(\mathrm{mod}\ n)$。

解密算法 恢复出明文$y^d=(m^e)^d=m^{ed}=m(\mathrm{mod}\ n)$。

2 RSA 算法中$\mathbf{Z}_{\varphi(n)}^*$的代数结构

众所周知:$\mathbf{Z}_{\varphi(n)}^*$在普通乘法模运算下构成一个群。而在 RSA 算法中,公钥e是在群$\mathbf{Z}_{\varphi(n)}^*$中选取的,私钥$d$就是$e$在群$\mathbf{Z}_{\varphi(n)}^*$中关于乘法模运算的逆元。在$p,q$为强素数条件下文献[6]对$\mathbf{Z}_n^*$的代数结构进行了研究,文献[7]在$p,q$为二阶强素数时对$\mathbf{Z}_{\varphi(n)}^*$的代数结构进行了研究,本文对$p,q$是强素数时$\mathbf{Z}_{\varphi(n)}^*$的代数结构作了进一步的研究。

收稿日期:2013-06-03;**修回日期**:2013-07-23。

作者简介:裴东林(1961-),男,甘肃兰州人,副教授,主要研究方向:密码学、应用数学; 李旭(1982-),男,甘肃天水人,讲师,博士研究生,主要研究方向:计算数学。

定义 1[7]　设 p,q 是两个奇素数且 $p \neq q$,如果 $p' = (p-1)/2, q' = (q-1)/2$ 均为大素数,则称 p,q 为强素数,如果 p,q 及 p',q' 均为强素数,则称 p,q 为二阶强素数。

显然,p,q 是二阶强素数时,p,q 必为强素数;反之不然,例如 $p = 263, q = 839$。

定理 1　在 RSA 算法中,若 $n = pq$ 且 p,q 为强素数,记 $p' = (p-1)/2, q' = (q-1)/2$,设元素 $a \in \mathbf{Z}_{\varphi(n)}^*$ 在 $\mathbf{Z}_4^*, \mathbf{Z}_{p'}^*, \mathbf{Z}_{q'}^*$ 中关于乘法模运算下的阶分别为 u,v,w,则元素 a 在 $\mathbf{Z}_{\varphi(n)}^*$ 中的阶为 $t = \mathrm{lcm}(u,v,w)$。

证明　由于 $\varphi(n) = (p-1)(q-1) = 4p'q'$ 且同余式 $a^u \equiv 1 (\mathrm{mod}\ 4)$, $a^v \equiv 1 (\mathrm{mod}\ p')$ 及 $a^w \equiv 1 (\mathrm{mod}\ q')$ 同时成立,因此,同余式 $a^t \equiv 1 (\mathrm{mod}\ \varphi(n))$ 也成立。

设 a 在 $\mathbf{Z}_{\varphi(n)}^*$ 中的阶为 t',可知 $t' \mid t$ 并且 $a^{t'} \equiv 1 (\mathrm{mod}\ \varphi(n))$,于是同余式 $a^{t'} \equiv 1 (\mathrm{mod}\ 4)$, $a^{t'} \equiv 1 (\mathrm{mod}\ p')$ 及 $a^{t'} \equiv 1 (\mathrm{mod}\ q')$ 同时成立[8],又因为 u,v,w 分别是元素 a 在 $\mathbf{Z}_4^*, \mathbf{Z}_{p'}^*, \mathbf{Z}_{q'}^*$ 中关于乘法模运算下的阶,故 $u \mid t', v \mid t', w \mid t'$,从而 $t \mid t'$,综上知 $t = t'$。

定理 2　在 RSA 算法中,若 $n = pq$ 且 p,q 为强素数,记 $p' = (p-1)/2, q' = (q-1)/2$,则在 $\mathbf{Z}_{\varphi(n)}^*$ 中所有元素的阶最大为 $t = \mathrm{lcm}(p'-1, q'-1)$ 且 $\mathbf{Z}_{\varphi(n)}^*$ 中所有元素的阶都是 t 的因子。

证明　设 $a \in \mathbf{Z}_{\varphi(n)}^*$,由于 $\varphi(n) = 4p'q'$,故 $a \in \mathbf{Z}_4^*, a \in \mathbf{Z}_{p'}^*, a \in \mathbf{Z}_{q'}^*$,根据欧拉定理知 $a^{p'-1} \equiv 1 (\mathrm{mod}\ p')$, $a^{q'-1} \equiv 1 (\mathrm{mod}\ q')$,又因为 $a \equiv \pm 1 (\mathrm{mod}\ 4)$,因此,同余式 $a^t \equiv 1 (\mathrm{mod}\ 4)$, $a^t \equiv 1 (\mathrm{mod}\ p')$, $a^t \equiv 1 (\mathrm{mod}\ q')$ 同时成立(注意 t 是偶数),因此 $a^t \equiv 1 (\mathrm{mod}\ \varphi(n))$[8],即 $\mathbf{Z}_{\varphi(n)}^*$ 中元素的阶不超过 t。

下面证明 $\mathbf{Z}_{\varphi(n)}^*$ 中存在阶为 t 的元素。

由于在普通乘法模运算下 $\mathbf{Z}_{p'}^*, \mathbf{Z}_{q'}^*$ 都是循环群,设 a,b 分别是 $\mathbf{Z}_{p'}^*, \mathbf{Z}_{q'}^*$ 的生成元,故知 a,b 在群 $\mathbf{Z}_{p'}^*, \mathbf{Z}_{q'}^*$ 中的阶分别为 $p'-1, q'-1$,作同余方程组 $x \equiv 1 (\mathrm{mod}\ 4)$, $x \equiv a (\mathrm{mod}\ p')$, $x \equiv b (\mathrm{mod}\ q')$。由中国剩余定理知上述同余方程组有唯一解记为 x_0,显然 x_0 在 $\mathbf{Z}_4^*, \mathbf{Z}_{p'}^*, \mathbf{Z}_{q'}^*$ 中关于乘法模运算下的阶分别为 $1, p'-1, q'-1$,根据定理 1 知 x_0 在 $\mathbf{Z}_{\varphi(n)}^*$ 中的阶为 $\mathrm{lcm}(1, p'-1, q'-1)$,即在 $\mathbf{Z}_{\varphi(n)}^*$ 中存在阶为 $\mathrm{lcm}(p'-1, q'-1)$ 的元素。对于任何 $a \in \mathbf{Z}_{\varphi(n)}^*$,由上述证明知 $a^t \equiv 1 (\mathrm{mod}\ \varphi(n))$,故 a 的阶是 t 的因子。

定理 3　在 RSA 算法中,若 $n = pq$ 且 p,q 为强素数,则在 $\mathbf{Z}_{\varphi(n)}^*$ 中模 $\varphi(n)$ 的二次剩余共有 $\varphi(\varphi(n))/8$ 个。

证明　设 a 是模 $\varphi(n)$ 的二次剩余,$\mathbf{Z}_{\varphi(n)}^*$ 中模 $\varphi(n)$ 的二次剩余组成的集合为:

$$\{a \mid x^2 \equiv a (\mathrm{mod}\ \varphi(n)), x \in \mathbf{Z}_{\varphi(n)}^*\}$$

显然 $\mathbf{Z}_{\varphi(n)}^*$ 中每个元素都是某个二次剩余的根。由于 $\varphi(n) = 4p'q'$,故同余式

$$x^2 \equiv a (\mathrm{mod}\ \varphi(n)) \tag{1}$$

与下列同余式组

$$x^2 \equiv a (\mathrm{mod}\ 4) \tag{2}$$

$$x^2 \equiv a (\mathrm{mod}\ p') \tag{3}$$

$$x^2 \equiv a (\mathrm{mod}\ q') \tag{4}$$

等价[8],而同余式(2)、(3)、(4)分别有两个根,所以,同余式(1)在 $\mathbf{Z}_{\varphi(n)}^*$ 中共有 8 个根[8],下面证明这 8 个根互不相等。

记同余式(2)、(3)、(4)的根分别是 $x_1, x_2; x_3, x_4; x_5, x_6$;根据中国剩余定理知:同余式组

$$x \equiv x_1 (\mathrm{mod}\ 4) \tag{5}$$

$$x \equiv x_3 (\mathrm{mod}\ p') \tag{6}$$

$$x \equiv x_5 (\mathrm{mod}\ q') \tag{7}$$

确定同余式(1)的唯一解。同理,用 $(x_1,x_4,x_5), (x_2,x_3,x_5), (x_2,x_4,x_5), (x_1,x_3,x_6), (x_1,x_4,x_6), (x_2,x_4,x_6), (x_2,x_3,x_6)$ 分别代替同余式组(5)、(6)、(7)中的 x_1,x_3,x_5,由此同余式组可分别确定同余式(1)的 7 个根。因此,同余式(1)的 8 个根不相等。故 $\mathbf{Z}_{\varphi(n)}^*$ 中每 8 个不相同的元素对应唯一的一个二次剩余,而 $\mathbf{Z}_{\varphi(n)}^*$ 中共有 $\varphi(\varphi(n))$ 个元素,故 $\mathbf{Z}_{\varphi(n)}^*$ 中的二次剩余共有 $\varphi(\varphi(n))/8$ 个。

定理 4　在 RSA 算法中,若 $n = pq, p,q$ 为强素数,$p' = (p-1)/2, q' = (q-1)/2$,则:1) 在 $\mathbf{Z}_{\varphi(n)}^*$ 中元素阶的最大可能为 $\varphi(\varphi(n))/4$;2) $\mathbf{Z}_{\varphi(n)}^*$ 中存在阶为 $\varphi(\varphi(n))/4$ 的元素的充要条件是 $\gcd(p'-1, q'-1) = 2$;若 a 的阶为 $\varphi(\varphi(n))/4$ 时,则 a 为模 $\varphi(n)$ 的二次非剩余。

证明

1) 根据定理 2 可知:存在 $a \in \mathbf{Z}_{\varphi(n)}^*$,$a$ 的阶为 $\mathrm{lcm}(p'-1, q'-1)$,由于 $\varphi(n) = 4p'q'$,故由欧拉函数计算公式可得:$\varphi(\varphi(n)) = 2(p'-1)(q'-1)$。

显然 $\mathrm{lcm}(p'-1, q'-1) = \dfrac{(p'-1)(q'-1)}{\gcd(p'-1, q'-1)} = \dfrac{\varphi(\varphi(n))}{2\gcd(p'-1, q'-1)}$,由于 $\gcd(p'-1, q'-1) \geqslant 2$,于是 a 的阶最大可能为 $\varphi(\varphi(n))/4$。

2) 若 $\gcd(p'-1, q'-1) = 2$,由上述证明知 a 的阶为 $\varphi(\varphi(n))/4$;反之,若 $\mathbf{Z}_{\varphi(n)}^*$ 中存在阶为 $\varphi(\varphi(n))/4$ 的元素,则 $\dfrac{\varphi(\varphi(n))}{2\gcd(p'-1, q'-1)} = \dfrac{\varphi(\varphi(n))}{4}$,从而 $\gcd(p'-1, q'-1) = 2$ 若 a 的阶为 $\varphi(\varphi(n))/4$,假设 a 为模 $\varphi(n)$ 的二次剩余,不难得知 $< a >$ 中元素均为二次剩余,由定理 3 可知:$|< a >| \leqslant \varphi(\varphi(n))/8$,显然与 a 的阶为 $\varphi(\varphi(n))/4$ 矛盾。

定理 5　在 RSA 算法中,若 $n = pq$ 且 p,q 为强素数,记 $p' = (p-1)/2, q' = (q-1)/2$,若 $\gcd(p'-1, q'-1) = 2$,则 $\mathbf{Z}_{\varphi(n)}^*$ 中全部二次剩余构成循环子群。

证明　显然 1 是 $\mathbf{Z}_{\varphi(n)}^*$ 中的二次剩余,设 a,b 为 $\mathbf{Z}_{\varphi(n)}^*$ 中的任意两个二次剩余,不难得知:ab 也是二次剩余,故在 $\mathbf{Z}_{\varphi(n)}^*$ 中全部二次剩余构成一个子群。由于 $\gcd(p'-1, q'-1) = 2$,根据定理 4 知:存在 $a \in \mathbf{Z}_{\varphi(n)}^*$ 的阶为 $\varphi(\varphi(n))/4$ 且 a 为模 $\varphi(n)$ 的二次非剩余,注意到 $\varphi(\varphi(n))/4$ 为偶数,从而不难推知:二次剩余 a^2 的阶为 $\varphi(\varphi(n))/8$,显然循环子群 $< a^2 > \subset \mathbf{Z}_{\varphi(n)}^*$ 的阶亦为 $\varphi(\varphi(n))/8$ 且 $< a^2 >$ 中元素均为二次剩余,根据定理 3 可知:$< a^2 >$ 生成了 $\mathbf{Z}_{\varphi(n)}^*$ 中的全部二次剩余是循环子群。

定理 6　在 RSA 算法中,若 $n = pq$ 且 p,q 为强素数,$p' = (p-1)/2, q' = (q-1)/2$,令

$$A_1 = \left\{a \mid a \in \mathbf{Z}_{\varphi(n)}^*, a \equiv 1 \bmod 4, \left(\frac{a}{p'}\right) = 1, \left(\frac{a}{q'}\right) = 1\right\}$$

$$A_2 = \left\{a \mid a \in \mathbf{Z}_{\varphi(n)}^*, a \equiv 1 \bmod 4, \left(\frac{a}{p'}\right) = -1, \left(\frac{a}{q'}\right) = 1\right\}$$

$$A_3 = \left\{a \mid a \in \mathbf{Z}_{\varphi(n)}^*, a \equiv 1 \bmod 4, \left(\frac{a}{p'}\right) = 1, \left(\frac{a}{q'}\right) = -1\right\}$$

$$A_4 = \left\{a \mid a \in \mathbf{Z}_{\varphi(n)}^*, a \equiv 1 \bmod 4, \left(\frac{a}{p'}\right) = -1, \left(\frac{a}{q'}\right) = -1\right\}$$

$$A_5 = \left\{a \mid a \in \mathbf{Z}_{\varphi(n)}^*, a \equiv -1 \bmod 4, \left(\frac{a}{p'}\right) = 1, \left(\frac{a}{q'}\right) = 1\right\}$$

$$A_6 = \left\{a \mid a \in \mathbf{Z}_{\varphi(n)}^*, a \equiv -1 \bmod 4, \left(\frac{a}{p'}\right) = -1, \left(\frac{a}{q'}\right) = 1\right\}$$

$$A_7=\left\{a\mid a\in \mathbf{Z}^*_{\varphi(n)},a\equiv -1 \bmod 4,\left(\frac{a}{p'}\right)=1,\left(\frac{a}{q'}\right)=-1\right\}$$

$$A_8=\left\{a\mid a\in \mathbf{Z}^*_{\varphi(n)},a\equiv -1 \bmod 4,\left(\frac{a}{p'}\right)=-1,\left(\frac{a}{q'}\right)=-1\right\}$$

则 $|A_i|=\varphi(\varphi(n))/8(i=1,2,\cdots,8)$,$A_1,A_2,A_3,\cdots,A_8$ 两两不相交且 $\bigcup_{i=1}^{8}A_i=\mathbf{Z}^*_{\varphi(n)}$,即 $A_1,A_2,A_3,\cdots,A_8$ 构成了 $\mathbf{Z}^*_{\varphi(n)}$ 的一个分割。

证明 对于任意元素 $b\in \mathbf{Z}^*_{\varphi(n)}$,由于 $\varphi(n)=4p'q'$,故 $b\equiv \pm 1(\bmod 4)$,$\left(\frac{b}{p'}\right)=\pm 1$ 及 $\left(\frac{b}{q'}\right)=\pm 1$ 都是唯一的,从而 b 必然属于且唯一属于以上 8 个集合之一,从而 $\bigcup_{i=1}^{8}A_i=\mathbf{Z}^*_{\varphi(n)}$,$A_1,A_2,A_3,\cdots,A_8$ 两两不相交且构成了 $\mathbf{Z}^*_{\varphi(n)}$ 的一个分割。

由二次剩余理论不难推知:在 $\mathbf{Z}^*_{\varphi(n)}$ 中,集合 A_1 包含了全部二次剩余,由定理 3 可知:$|A_1|=\varphi(\varphi(n))/8$,从而二次非剩余共有 $\sum_{i=2}^{8}|A_i|=\frac{7}{8}\varphi(\varphi(n))$。任取一个二次非剩余,不妨设 $x_0\in A_2$,用 $x_0\mathbf{Z}^*_{\varphi(n)}$ 表示 x_0 乘以 $\mathbf{Z}^*_{\varphi(n)}$ 所构成的集合。由于 $\mathbf{Z}^*_{\varphi(n)}$ 是一个乘法群,元素与元素的积封闭,$x_0\mathbf{Z}^*_{\varphi(n)}\subseteq \mathbf{Z}^*_{\varphi(n)}$;反之,对于任意的元素 $a_1,a_2\in \mathbf{Z}^*_{\varphi(n)}$,如果 $x_0a_1=x_0a_2$,两边同乘以 $x_0^{-1}\in \mathbf{Z}^*_{\varphi(n)}$ 可知 $a_1=a_2$,也就是说,$x_0\mathbf{Z}^*_{\varphi(n)}$ 中的元素和 $\mathbf{Z}^*_{\varphi(n)}$ 的元素一样多,故可知 $x_0\mathbf{Z}^*_{\varphi(n)}=\mathbf{Z}^*_{\varphi(n)}$。对于集合 $x_0\mathbf{Z}^*_{\varphi(n)}$ 来说,任取元素 $x\in A_2$,由于 $xx_0\equiv 1(\bmod 4)$,$\left(\frac{x\cdot x_0}{p'}\right)=\left(\frac{x}{p'}\right)\left(\frac{x_0}{p'}\right)=(-1)\times(-1)=1$,$\left(\frac{x\cdot x_0}{q'}\right)=\left(\frac{x}{q'}\right)\left(\frac{x_0}{q'}\right)=1$,故 $x_0A_2\subseteq A_1$,从而有 $|x_0A_2|=|A_2|\leqslant|A_1|$。

对于集合 x_0A_1 来说,任取元素 $a\in A_1$,由于 $a\cdot x_0\equiv 1(\bmod 4)$,$\left(\frac{a\cdot x_0}{p'}\right)=\left(\frac{a}{p'}\right)\left(\frac{x_0}{p'}\right)=(-1)\times(-1)=1$,$\left(\frac{a\cdot x_0}{q'}\right)=\left(\frac{a}{q'}\right)\left(\frac{x_0}{q'}\right)=1$,因此,$x_0a\in A_2$,故 $x_0A_1\subseteq A_2$,从而有 $|x_0A_1|=|A_1|\leqslant|A_2|$,所以有 $|A_1|=|A_2|$。

同理可证:$|A_i|=|A_1|(i=3,4,\cdots,8)$,总之 $|A_i|=\varphi(\varphi(n))/8(i=1,2,\cdots,8)$。

定理 7 在 RSA 算法中,若 $n=pq$ 且 p,q 为强素数,$p'=(p-1)/2,q'=(q-1)/2$,$p'-1=2s,q'-1=2t$,且 s,t 为奇数,则 $\mathbf{Z}^*_{\varphi(n)}$ 可由 7 个二次非剩余元素生成。

证明 根据定理 6,知:$\mathbf{Z}^*_{\varphi(n)}=\bigcup_{i=1}^{8}A_i$ 构成了 $\mathbf{Z}^*_{\varphi(n)}$ 的分割,由于 s,t 为奇数,故 $\gcd(p'-1,q'-1)=2$,从而由 A_1 的定义及定理 3、定理 5 及定理 6 不难推知:A_1 是 $\mathbf{Z}^*_{\varphi(n)}$ 中全部二次剩余构成的循环子群,又根据定理 4 知:在 $\mathbf{Z}^*_{\varphi(n)}$ 中存在阶为 $\varphi(\varphi(n))/4$ 的元素且该元素为模 $\varphi(n)$ 的二次非剩余,记这样的元素为 x_1,则 $x_1\notin A_1$,不妨设 $x_1\in A_2$,显然 $<x_1>$ 是阶为 $\varphi(\varphi(n))/4$ 的循环子群,由 A_2 的定义不难推知:对任意整数 m,有 $x_1^{2m}\in A_1,x_1^{2m+1}\in A_2$,从而 $<x_1>\subseteq(A_1\cup A_2)$,但 $|<x_1>|=\left|(A_1\cup A_2)\right|=\varphi(\varphi(n))/4$,于是 $<x_1>=A_1\cup A_2$。

记 $a=x_1^2(\bmod \varphi(n))$,显然 $<a>=A_1$,根据定理 3 的证明知:同余方程 $x^2\equiv a(\bmod \varphi(n))$ 共有 8 个互不相同的根,这 8 个根中除 x_1 外的其余 7 个根分别记为 $x_2,x_3,x_4,x_5,x_6,x_7,x_8$,下面证明它们分别属于 $A_1,A_3,A_4,\cdots,A_8$。如若不然,则在它们中至少存在两个元素同时属于 $A_1,A_3,A_4,\cdots,A_8$ 中的某一个集合,记这样的两个元素分别为 $x',x''\in A_k(1\leqslant k\leqslant 8,k\neq 2)$,由 A_k 的定义不难得知:$x'x''\in A_1$,由于 $<a>=A_1$,故存在整数 m,使得 $x'x''=a^m$,于是,不难推知 $a^2=a^{2m}$,因此 $a^{2(m-1)}\equiv 1(\bmod \varphi(n))$,从而 $|<a>|\,|2(m-1)$,由于 $|<a>|=\varphi(\varphi(n))/8=st$,而 s,t 均为奇数,所以 $\gcd(|<a>|,2)=1$,从而有 $|<a>|\,|(m-1)$,即 $m\equiv 1(\bmod |<a>|)$,因此,$x'x''=a^m\equiv a(\bmod \varphi(n))$,即 $x'x''\equiv a(\bmod \varphi(n))$,由此可得 $x'x''=x'^2$,从而得出 $x'\equiv x''(\bmod \varphi(n))$,这与 x',x'' 是不相同的根相矛盾。因此,$x_i\in A_i(i=3,4,\cdots,8)$,又 A_1 是 $\mathbf{Z}^*_{\varphi(n)}$ 中全部二次剩余构成的循环子群,所以,$x_i(i=3,4,\cdots,8)$ 均为二次非剩余。

由于 $x_i\in A_i$ 且 $x_i^2=a(i=3,4,\cdots,8)$,从而 $|<a>|<|<x_i>|$,因为 $|<a>|=\varphi(\varphi(n))/8$,故不难得知二次非剩余 x_i 的阶均为 $\varphi(\varphi(n))/4$,由 A_i 的定义不难推知:对任意整数 m,有 $x_i^{2m}\in A_1,x_i^{2m+1}\in A_i$,从而 $<x_i>\subseteq(A_1\cup A_i)$,但 $|<x_i>|=\left|(A_1\cup A_i)\right|=\varphi(\varphi(n))/4$,于是 $<x_i>=A_1\cup A_i$。综上可知 $\mathbf{Z}^*_{\varphi(n)}=<x_1,x_3,x_4,x_5,x_6,x_7,x_8>$。

定理 8 在 RSA 算法中,若 $n=pq$ 且 p,q 为强素数,记 $p'=(p-1)/2,q'=(q-1)/2$,若 $\gcd(p'-1,q'-1)=2$,则 A_1 是 $\mathbf{Z}^*_{\varphi(n)}$ 中的不变子群,并且由子群 A_1 在 $\mathbf{Z}^*_{\varphi(n)}$ 做成的陪集刚好是 $A_1,A_2,A_3,A_4,A_5,A_6,A_7,A_8$。由陪集做成的商群 $\mathbf{Z}^*_{\varphi(n)}/A_1$ 是一个 Klein 八元群(A_i 的意义见定理 6)。

证明 由于 $\gcd(p'-1,q'-1)=2$,根据定理 5 知:A_1 是 $\mathbf{Z}^*_{\varphi(n)}$ 的循环子群,又因为 $\mathbf{Z}^*_{\varphi(n)}$ 中元素对乘法模运算满足交换律,所以,A_1 是 $\mathbf{Z}^*_{\varphi(n)}$ 中的不变子群。任取 $x_i\in A_i(i=1,2,\cdots,8)$,易知 $x_iA_1=A_i(i=1,2,\cdots,8)$,从而由子群 A_1 在 $\mathbf{Z}^*_{\varphi(n)}$ 中作成的陪集刚好是 $A_1,A_2,A_3,A_4,A_5,A_6,A_7,A_8$,故商群 $\mathbf{Z}^*_{\varphi(n)}/A_1$ 是一个八元群。

下面证明商群 $\mathbf{Z}^*_{\varphi(n)}/A_1$ 中每个元素的阶都是 2。

在陪集中定义乘法如下:

对于任意的 $u,v\in \mathbf{Z}^*_{\varphi(n)}$,规定 $uA_1\circ vA_1=uvA_1$。由上述分析知:此定义对新的乘法是合理的。容易看到 A_1 是商群 $\mathbf{Z}^*_{\varphi(n)}/A_1$ 中的单位元,又因为对于任意的 $u\in \mathbf{Z}^*_{\varphi(n)}$,$u\cdot u\in A_1$,从而就有 $x_iA_1\circ x_iA_1=A_1(i=2,3,\cdots,8)$,即 $\mathbf{Z}^*_{\varphi(n)}/A_1$ 中除单位元外每个元素的阶都是 2。

综上可知:商群 $\mathbf{Z}^*_{\varphi(n)}/A_1$ 是一个 Klein 八元群。

3 结语

RSA 算法是近 30 年来备受数学界、密码学界关注的一个问题,近年来,通过研究加解密算法的代数结构并由此分析其安全性的方法引起了许多研究者的兴趣,由此产生的代数攻击逐渐成为密码分析中的热点,出现了大量的对于分组密码、流密码、公钥密码的研究成果[9-13]。本文通过对 RSA 算法代数结构研究发现:在强素数条件下,群 $\mathbf{Z}^*_{\varphi(n)}$ 仍有许多良好的性质,这些性质对分析 RSA 的安全性是有意义的,比如对 RSA 进行循环攻击时,公钥 e 在群 $\mathbf{Z}^*_{\varphi(n)}$ 中的阶越大,则完全攻破 RSA 就越困难;反之就比较容易。今后,将对 RSA 算法中 p,q 不是强素数的情况下 RSA 的代数结构进行研究并利用 RSA 的代数结构对其各类攻击进行分析。

(下转第 3266 页)

第 3 步　依据控制流图生成基本路径集。

对于较复杂的程序,需要花费较长的设计时间,设计效率比较低。

3)基本路径组合法算法实现简单。

在基本路径组合法中,采用堆栈数据结构即可实现第 1 步,即分析程序结构得基本子路径集。第 2 步实际上是按组合方式进行字符串的组合,因此,只需要采用基本的程序设计技术就能实现。

比较而言,McCabe 法算法实现较难,虽然文献[1-2]用算法实现了 McCabe 方法的 3 个步骤,但文献[1]不支持多分支结构,文献[2]采用了符号测试法选择基本路径集,执行效率低下,目前为止还没有算法能较完整地实现 McCabe 提出的方法。

3　结语

本文提出了一种基本路径测试用例设计的新算法,该算法有别于 McCabe 的思路,从被测程序的结构出发,只需要一次扫描被测程序得到其包含的基本子路径集,最后,按照组合规则将这些子路径进行组合,即可得到被测程序的基本路径集。目前,本研究实现了针对 C#代码的基本子路径集生成、基本路径集求解和基于基本路径测试的程序插桩版的生成。在后续的研究中,将借助于该算法的思想,进一步以工具的形式实现基本路径测试全过程的自动化,包括基本路径集的自动生成、测试数据的自动生成、测试用例的自动执行及测试报告的自动生成。本次讨论的对象没有考虑条件拆分的情况,也将在后续研究中完善。

参考文献:

[1] WIJAYASIRIWARDHANE T K, WIJAYARATHNA P G, KARUNARATHNA D D. An automated tool to generate test cases for performing basis path testing [C]// ICTer 2011: Proceedings of the 2011 International Conference on Advances in ICT for Emerging Regions. Piscataway: IEEE Press, 2011: 95 - 101.

[2] 严俊,郭涛,阮辉,等. JUTA: 一个 Java 自动化单元测试工具[J]. 计算机研究与发展,2010,47(10):170 - 178.

[3] 解圣霞. 基于基本路径测试的程序图自动生成的应用研究[J]. 通化师范学院学报,2009,30(12):38 - 41.

[4] ZHANG Z L, MEI L X. An improved method of acquiring basis path for software testing [C]// Proceedings of the 5th International Conference on Computer Science and Education. Piscataway: IEEE Press, 2010: 1891 - 1894.

[5] 王冠,景小宁,王彦军. 基本路径测试中的 McCabe 算法改进与应用[J]. 哈尔滨理工大学学报. 2010,15(1):48 - 51.

[6] 毛澄映,卢炎生. 分支测试中测试路径用例的简化生成方法[J]. 计算机研究与发展,2006,43(2):321 - 328.

[7] DU Q F, DONG X. An improved algorithm for basis path testing [C]// Proceedings of the 2011 International Conference on Business Management and Electronic Information. Piscataway: IEEE Press, 2011: 175 - 178.

[8] 杜庆峰,李娜. 白盒测试基本路径算法[J]. 计算机工程,2009,35(15):100 - 102.

[9] McCABE T J. A complexity measure [J]. IEEE Transactions on Software Engineering, 1976, SE-2(4): 308 - 320.

[10] 佟伟光. 软件测试[M]. 北京: 人民邮电出版社,2008:60 - 61.

[11] LUN L J, CHI X. Path numbers analysis of relationships on software architecture testing criteria [C]// Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering. Piscataway: IEEE Press, 2010: 118 - 122.

[12] 王培崇,钱旭. 基于改进鱼群算法的路径测试数据生成[J]. 计算机应用,2013,33(4):1139 - 1141.

[13] 施冬梅. 基本路径覆盖测试探针插桩技术研究[J]. 计算机工程与设计,2010,31(13):3025 - 3028.

[14] YANGU Y J, LUN L J, CHI X. Research on path generation for software architecture testing matrix transform-based [C]// CSSS 2011: Proceedings of the 2011 International Conference on Computer Science and Service System. Piscataway: IEEE Press, 2011: 2483 - 2486.

(上接第 3246 页)

参考文献:

[1] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public key crypto systems [J]. Communications of the ACM, 1978, 21(2): 120 - 126.

[2] BONEH D. Twenty years of attacks on the RSA cryptosystem [J]. Notices of the AMS, 1999, 46(2): 203 - 212.

[3] LENSTRA A K. Integer factoring [J]. Designs Codes and Cryptography, 2000, 19: 101 - 128.

[4] SHAMA S, SHAMA P, DHAKAR R S. RSA algorithm using modified subset sum cryptosystem [C]// ICCCT-2011: Proceedings of the 2011 International Conference on Computer and Communication Technology. Piscataway: IEEE Press, 2011: 457 - 461.

[5] BELLARE M, NEVEN G. Identity based multi signatures from RSA [C]// Proceedings of the 7th Cryptographers' Track at the RSA Conference on Topics in Cryptology. Berlin: Springer-Verlag, 2007: 145 - 162.

[6] 司光东,杨加喜,谭示崇,等. RSA 算法中的代数结构[J]. 电子学报,2011,39(1):242 - 246.

[7] 裴东林,胡建军,李旭. RSA 算法中$\mathbf{Z}_{\varphi(n)}^{*}$的代数结构研究[J]. 计算机工程,2013,39(2):145 - 149.

[8] 闵嗣鹤,严士健. 初等数论[M]. 3 版. 北京: 高等教育出版社,2003.

[9] RIZOMILIOTIS P. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation [J]. IEEE Transactions on Information Theory, 2010, 56(8): 4014 - 4024.

[10] KNUDSEN L R, MIOLANE C V. Counting equations in algebraic attacks on block ciphers [J]. International Journal of Information Security, 2010, 9(2): 127 - 135.

[11] GHOSH S, DAS A. An improvement of linearization-based algebraic attacks [C]// Proceedings of the First International Conference on Security Aspects in Information Technology. Berlin: Springer-Verlag, 2011: 157 - 167.

[12] 谢佳,王天择. 寻找布尔函数的零化子[J]. 电子学报,2010,38(11):2686 - 2690.

[13] 李昕,林东岱. 对 Bivium 流密码的变元猜测代数攻击[J]. 电子学报,2011,39(8):1727 - 1732.