关于 II 型安全素数的探讨*

余启港**

（中南民族大学，湖北，武汉 430074）

摘要 定义了 II 型安全素数，关联 II 型安全素数序列和 n 重 II 型安全素数，给出了他们各自的判别条件，并证明了 n 重 II 型安全素数重数的有限性，最后提出了两个关于 n 重安全素数重数上界的猜想。

关键词 II 型安全素数；关联 II 型安全素数序列；n 重 II 型安全素数；RSA 密码体制。

MR（1991）主题分类 11D61

中图分类号 O156 **文献标识码** A **文章编号**

Discuss on the II-form safe prime number

Yu Qigang

(Zhongnan Minzu Daxue of Hubei ,Wuhan 430074 , P.R.China)

Abstract **Definited II-form safe prime number,related II-form safe prime number sequence and n co-II-form safe prime number , goven its-self-each discrite condition ,proved finity of order of n co-II-form safe prime number . Finally, moken two conjections of upper bound of order of n co-form safe prime number .**

Keywords II-form **safe prime number ; relative** II-form **safe prime number serier ; n co-II-form safe prime number ; RSA cyptosystem.**

MR（1991）Subject Classification **11D61**

Chinese Library Classification **O156.5**

RSA 密码应用需要大量的大素数对，且由于对抗密码分析的需要，大素数须满足一定的条件。例如，对抗“$p-1$ 法 ”分析，人们定义了安全素数：当 p 和 $q=2p-1$ 都是素数时，称 q 为安全素数。有大量的文献讨论了这种安全素数的密码学性质。高宏老师和我们也对这种安全素数进行过一些研究[1-4]。本文从对抗“$p+1$ 法” 分析的角度，提出了另一种安全素数的概念（称为 II 型安全素数），并进行了与我们前期工作相似的一些讨论, 如只利用幂模运算生成 II 型安全素数等。

1 定义

定义 1 设 p 是素数，若 $q=2p-1$ 也是素数，则称 q 是 II 型安全素数，并称通常的安全素数为 I 型安全素数。

定义 2 设 p_0 是素数，如果 $p_k=2p_{k-1}-1,k=1,\cdots,n$ 都是素数，则称 $\{p_k\}_{k=1}^{n}$ 是由 p_0 生成的关联 II 型安全素数序列，特别称 p_n 是由 p_0 生成的 n 重 II 型安全素数。

显然，$p_k,k=1,\cdots,n$ 都是 II 型安全素数。

通过求解递推关系 $p_k=2p_{k-1}-1,k=1,\cdots,n$，易得 $p_k=2^k p_0-2^k+1,k=1,\cdots,n$。

2 $Lacus$ 序列的计算

下节判别方法中用到 $Lacus$ 序列：

设 P 和 Q 为非零整数，且多项式 x^2-Px+Q 的判别式 $D=P^2-4Q\neq 0$。记其两根分别为 α 和 β，即 $\alpha=\dfrac{P+\sqrt{D}}{2},\beta=\dfrac{P-\sqrt{D}}{2}$。令 $U_n=U_n(P,Q)=\dfrac{\alpha^n-\beta^n}{\alpha-\beta}$, $V_n=V_n(P,Q)=\alpha^n+\beta^n$, 则 $U_0=0,U_1=1,V_0=2,V_1-P.$

* 项目资助：国家民委重点研究项目（980101）和中南民族大学自然科学基金研究项目（20010101）

** 作者简介：余启港，男，1962 年 4 月生。中南民族大学计算机科学学院副教授，主要从事数论与密码学的研究和线性代数的教学研究。

记 $n=n_0 2^k+n_1 2^{k-1}+\cdots+n_k$，其中 $n_i=0$ 或 $1,(i=1,\cdots,k)$ 且 $n_0=1.$ 记 $s_0=n_0=1,s_{j+1}=2s_j+n_{j+1}$,则 $s_k=n,U_{s_{j+1}}=U_{2s_j}$ 或 U_{2s_j+1},$V_{s_{j+1}}=V_{2s_j}$ 或 V_{2s_j+1} 再利用下述 $Lacus$ 序列的性质：$U_{2j}=U_jV_j$，$V_{2j}=V_J^2-2Q^j$，$2V_{2j+1}=V_{2j}+PU_{2j}$，$2V_{2j+1}=PV_{2j}+DU_{2j}$ 可计算 U_n 和 V_n.

另一种计算 U_n 和 V_n 的方法也非常快：由 $Lacus$ 序列的性质：$U_{j+1}=PU_j-QU_{j-1}$，$V_{j+1}=PV_j-QV_{j-1}$，有 $\begin{pmatrix} U_{j+1} & V_{j+1} \\ U_j & V_j \end{pmatrix}=\begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}\begin{pmatrix} U_j & V_j \\ U_{j-1} & V_{j-1} \end{pmatrix}$，记 $M=\begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}$，则递归可得 $\begin{pmatrix} U_n & V_n \\ U_{n-1} & V_{n-1} \end{pmatrix}=M^{n-1}\begin{pmatrix} 1 & P \\ 0 & 2 \end{pmatrix}$，而 M^m 可由 m 的二进制形式，通过“平方乘”方法快速算出。

如果求 $U_n(mod\,N)$ 和 $V_n(mod\,N)$，则在上述计算 U_n 和 V_n 过程中，每一步取 $mod\,N$ 代替即可。

3　II 型安全素数判别方法

设 p 为奇素数，$q=2p-1$。利用 $Lacus$ 序列理论[5]中的素性检测方法较易得到下述几个判别 q 为素数的结论。

定理 1　存在非零整数 P,Q 使下列条件满足时，q 为素数。

（1）$gcd(P,q)=1$。

（2）$gcd(P,Q)=1$ 或者 $gcd(q,Q)=1.$

（3）$D=P^2-4Q\neq 0$ 且 $Jacobi$ 符号 $\left(\dfrac{D}{q}\right)=-1.$

（4）$U_{2p}(P,Q)\equiv 0(mod\,q).$

定理 2　存在非零整数 P,Q 使下列条件满足时，q 为素数。

（1）$P\equiv 0(mod\,q).$

（2）$gcd(P,Q)=1$ 或者 $gcd(q,Q)=1.$

（3）$D=P^2-4Q\neq 0$ 且 $Jacobi$ 符号 $\left(\dfrac{D}{q}\right)=-1.$

（4）$V_p(P,Q)\equiv 0(mod\,q).$

4　同时抵抗“$p-1$ 攻击”和“$p+1$ 攻击”安全素数的生成算法

定理 3　p_0 为奇素数时，$q=4p_0+1$ 为素数的充分必要条件是 $3^{4p_0}\equiv 1(mod\,q)$ 且 $p_0\not\equiv 1(mod 10)$。

证明 必要性显然。

下证充分性。由 $p_0\not\equiv 1(mod 10)$ 知奇数 $q=4p_0+1\not\equiv 0(mod 5).$ 从而 $gcd(3^4-1,q)=gcd(2^4\times 5,q)=1.$ 再由条件 p_0 为奇素数且 $3^{4p_0}\equiv 1(mod\,q)$，根据

$Rockington\ H.C.(1916)$判别法[5]知q为素数。证毕。

定理 4 设p_0为奇素数且$p_0 \not\equiv 1(mod 10)$。再设$p_1 = 2p_0 + 1$，$p_2 = 2p_1 - 1 = 4p_0 + 1.$ 则p_1和p_2皆为素数的充分必要条件是（1）$2^{2p_0} \equiv 1\ \ (mod\ p_1).$（2）$3^{4p_0} \equiv 1(mod\ p_2).$

证明 当p_0为奇素数时，由文[1]知p_1为素数的充分必要条件是（1）$2^{2p_0} \equiv 1\ (mod\ p_1).$当$p_0$为奇素数且$p_0 \not\equiv 1(mod 10)$时，由上面定理 3 知$p_2$为素数的充分必要条件是（2）$3^{4p_0} \equiv 1(mod\ p_2).$证毕。

注 由于$p_2 - 1 = 4p_0, p_2 + 1 = 2p_1$，故用$p_2$作 RSA 密码的保密密钥，既可抵抗“$p-1$攻击”又可抵抗“$p+1$攻击”。

5 n重 II 型安全素数——重数的有限性

仿n重 I 型安全素数—重数的有限性[4]]的证明方法，利用关系式$p_k = 2^k p_0 - 2^k + 1, k = 1, \cdots, n$可证：

定理 5 设p_0是素数，p_n是由p_0生成的n重 II 型安全素数的必要条件是：$2^k \not\equiv 1(mod\ p_0), k = 1, \cdots, n.$

若记奇素数p_0生成的n重 II 型安全素数的重数的最大值为$PG(p_0)$，则$PG(p_0) < p_0 - 1$。我们还引进过[4]素数p_0生成的n重（I 型）安全素数的重数的最大值为$PF(p_0)$，同样有$PF(p_0) < p_0 - 1$。我们还易得到下述简单事实：设p_0是奇素数，则（1）$p_0 \not\equiv 29(mod 30)$时，$PF(p_0) \le 3.$（2）$p_0 \not\equiv 1(mod 30)$时$PG(p_0) \le 2$。

最后，我们提出如下两个猜想：

猜想 1 存在确定常数PF，使$PF(p_0) \le PF$对任何素数p_0都成立。

猜想 2 存在确定常数PG，使$PG(p_0) \le PG$对任何素数p_0都成立。

参考文献

[1]余启港，雷建云。安全素数的快速算法（J）中南民族学院学报（自然科学版）1999。Vol.19,No.2,45~47

[2] 余启港，雷建云。安全素数的快速算法的实现（J）中南民族学院学报（自然科学版）1999。Vol.19,No.2,23~26

[3] 高宏，汤学明，龚广飞。双重关联素数及其密码学性质（J）第五届中国密码学学术会议论文集，科学出版社，1998

[4] 余启港，张军好，雷建云。重安全素数的有限性（J）中南民族学院学报（自然科学版）2000。Vol

[5] Paulo Ribenboim, Handbook of Prime Number Records(Second Edition).Springer-Verlag.1989.