1999 年 6 月 通 信 学 报 Vol. 20 No. 6
第 20 卷 第 6 期 JOURNAL OF CHINA INSTITUTE OF COMMUNICATIONS June 1999

学术论文

关于有限域$\mathbb{F}_p$上多项式 RSA 的安全性和 RSA 的新模拟*

曹珍富**
(哈尔滨工业大学数学系 哈尔滨 150001)

摘 要 本文首先指出有限域F_p上多项式 RSA 是不安全的,然后给出了 RSA 在$\Sigma_r(r=pq)$中的两个新模拟。两个新体制的安全性将主要基于大整数的分解。

关键词 RSA 安全性 分解 有限域上的多项式
分类号 O151.26

On the Security of the RSA Based on a Polynomial Over Finite Fields $\mathbb{F}_p$ and a New Analog of the RSA

Cao Zhenfu
(Department of Mathematics, Harbin Institute of Technology, Harbin 150001)

Abstract First, we show that the RSA based on a polynomial over finite fields F_p is not secure. Next, we presents a new analog of the RSA. The security of the new cryptosystems main based on the factorization of large integers.

Key words RSA, security, factorization, polynomial over finite field

RSA 是 1978 年由 Rivest、Shamir 和 Adleman[1]提出的部分基于大整数分解的著名的公钥密码体制。自此以后,先后出现了对这一体制在不同范畴的各种模拟[2,3],例如,孙琦[4]、本文作者[5]和 Williams[6]等人考虑了 RSA 在代数整数环中的模拟,特别是在 Eisenstein 环$\Sigma[\omega]$和一般的二次域中的模拟。这种模拟无疑是对现代密码学的新贡献。

对 RSA 其它形式的模拟还可参看文[7,8]。在文献[7]中,孙琦提出了有限域$\mathbb{F}_p$(p 为素数)上多项式形式的 RSA。本文将指出,这种形式的 RSA 无论从哪个角度看均是不安全的。本文还将提出 RSA 的一个新模拟,新体制的安全性将主要基于大整数的分解。

1 有限域$\mathbb{F}_p$上多项式形式 RSA 的安全性

设 p 为素数,$\mathbb{F}_p$为 p 元有限域,$\mathbb{F}_p^*$为$\mathbb{F}_p$的乘群,不失一般性,设

$$\mathbb{F}_p=\{0,1,\cdots,p-1\},\ \mathbb{F}_p^*=\mathbb{F}_p\setminus\{0\}$$

$\mathbb{F}_p$上多项式形式 RSA 是基于$\mathbb{F}_p$上多项式的一个已知定理[3,7],写成下面的定理 1

定理 1 设$\mathbb{F}_p[x]$为$\mathbb{F}_p$上多次式环,$g(x)=g_1^{l_1}(x)\cdots g_k^{l_k}(x)\in\mathbb{F}_p[x]$是一个 m 次多项式,这里 $l_i\geqslant 1$,$g_i(x)$是$\mathbb{F}_p$上的 m_i 次不可约多项式($i=1,\cdots,k$)记

* 国家自然科学基金资助项目 批准号:69772037

** 曹珍富:男,1962 年生,教授,研究数论、现代密码学与数论对相关数学领域的应用

$$\varphi_p(g(x))=p^m\prod_{i=1}^{k}\left(1-\frac{1}{p^{m_i}}\right)$$

则对任何 $u(x)\in\mathbb{F}_p[x]$，只要 $u(x)$ 的次数大于 0 且 $(u(x),g(x))=1$，均成立

$$(u(x))^{\varphi_p(g(x))}\equiv 1(\bmod\ g(x))$$

为了便于分析 $\mathbb{F}_p$ 上多项式形式的 RSA，我们简要的介绍一下文[7]中体制的构成（这种体制简记为 $\mathbb{F}_p[x]$ −RSA）。

设 n 是一个正整数，p 是一个素数，将

$$n=a_hp^h+a_{h-1}p^{h-1}+\cdots+a_0,a_h\in\mathbb{F}_p,a_i\in\mathbb{F}_p\ (i=0,1,\cdots,h-1)$$

简记为 $n=[a_h,a_{h-1},\cdots,a_0]_p$，并称为 n 的 p−adic 形式，h 称为其长度。先取 $\mathbb{F}_p$ 上的一个 m 次多项式

$$g(x)=g_1^{l_1}(x)\cdots g_k^{l_k}(x),l_i\geqslant 1(i=1,\cdots,k),$$

这里 $g_i(x)$ 是 $\mathbb{F}_p$ 上的 m_i 次不可约多项式 $(i=1,\cdots,k)$，并选取 e 满足 $1<e<\varphi_p(g(x))$，$(e,\varphi_p(g(x)))=1$

计算 d 使其满足

$$ed\equiv 1(\bmod\ \varphi_p(g(x))),1<d<\varphi_p(g(x))$$

于是 $\{e,g(x)\}$ 公开，$\{d,\varphi_p(g(x))\}$ 保密，其加密、解密算法为：

加密：设 $[1,M]$ 为明文空间，$\partial(M)<m$，这里 $\partial(M)$ 是 M 的 p−adic 形式的长度。任意 $n\in[1,M]$，将 n 写成 $n=[a_h,a_{h-1},\cdots,a_0]_p$，在 $\mathbb{F}_p$ 上计算

$$\langle(a_hx^h+a_{h-1}x^{h-1}+\cdots+a_0)^e\rangle_{g(x)}=b_tx^t+\cdots+b_1x+b_0$$

这里符号 $\langle f(x)\rangle_{g(x)}$ 表示 $\mathbb{F}_p$ 上多项式 $f(x)$ 模 $g(x)$ 的余式，将 $[b_t,b_{t-1},\cdots,b_0]_p=c$ 作为密文。

解密：在 $\mathbb{F}_p$ 上计算

$$\langle(b_tx^t+b_{t-1}x^{t-1}+\cdots+b_0)^d\rangle_{g(x)}=a_hx^h+\cdots+a_1x+a_0,$$

因而恢复了明文 $n=[a_h,a_{h-1},\cdots,a_0]_p$

注 1 文献[7]要求“选择 m 次多项式 $g(x)$ 使得对任意 $n\in[1,M]$，$n=[a_h,a_{h-1},\cdots,a_0]_p$ 均有 $(g(x),a_hx^h+a_{h-1}x^{h-1}+\cdots+a_0)=1$”这是很难做到的，实际上是不必要的（只要在 $g(x)$ 的表达式中将每个 l_i 取为 1 即可）。

下面我们指出，$\mathbb{F}_p[x]$−RSA 体制是不安全的为此，引入 Berlekamp 给出的分解 $\mathbb{F}_p[x]$ 中多项式的标准算法的复杂性结果[9]。

定理 2 分解 $\mathbb{F}_p$ 上 n 次多项式的工作量为 $O(pn^3)$

在 $\mathbb{F}_p[x]$−RSA 体制中，如果 p 选取较小，由定理 2 知，在 $\mathbb{F}_p[x]$ 中分解 $g(x)$ 的工作量仅为 $O(m^3)$ 所以此时体制是不安全的，如果 p 选取十分巨大（例如 100 位左右的大素数），则 Berlekamp 算法对分解 $g(x)$ 没有任何意义，但当 p 选取很大时，多项式 $g(x)$ 的次数 m 就不能选取太大，不然 $\varphi_p(g(x))$ 将是十分巨大的（是 ∞^∞ 型），因而无法完成 e,d 的选取与计算，更难以用于加密与解密运算。如果 $g(x)$ 的次数不够大，由于 $g(x)$ 公开，则可对 $g_i(x)$ 的次数进行穷举来计算 $\varphi_p(g(x))$，由此可知，此时在不分解 $g(x)$ 的条件下亦可破译 $\mathbb{F}_p[x]$−RSA 体制。

总之，$\mathbb{F}_p[x]$−RSA 体制是不安全的。

注 2 文献[7]曾建议在 $\mathbb{F}_p[x]$−RSA 体制中取 $p=2,l_i=1(i=1,\cdots,k)e=2$，但这种情形是最不安全的，直接由定理 2 就可破译 $\mathbb{F}_p[x]$−RSA 体制。

2 RSA 的一个新模拟 RSAC1

在这一节我们提出一个 RSA 的新模拟 RSAC1，新体制的安全性将主要基于大整数的分

解，它是$\mathbb{F}_p[x]$－RSA 体制的一个改进。

现在给出新体制的构成。

设 p,q 均为大素数，$p<q$，$r=pq$，选取$\mathbb{F}_p$（因而$\mathbb{F}_q$）上的一个 m 次多项式 $g(x)$，使得在$\mathbb{F}_p$上有分解式

$$g(x)=g_1(x)\cdots g_k(x),$$

这里 $g_i(x)$是$\mathbb{F}_p$上的 m_i 次不可约多项式$(i=1,\cdots,k)$；在$\mathbb{F}_q$上有分解式

$$g(x)=g_1'(x)\cdots g_{k'}'(x),$$

这里 $g_i'(x)$是$\mathbb{F}_q$上的 m_i' 次不可约多项式$(i=1,\cdots,k')$。于是新体制的明文空间为$\mathbb{Z}_r^m$，密文空间为$\mathbb{Z}_r^{2m}$，这里$\mathbb{Z}_r$是模 r 的整数剩余类环。从 $g(x)$可以很容易计算出

$$\varphi_p(g(x))=p^m\prod_{i=1}^{k}\left(1-\frac{1}{P^{m_i}}\right),\varphi_q(g(x))=q^m\prod_{i=1}^{k'}\left(1-\frac{1}{q^{m_i'}}\right)$$

用 Euclid 算法容易求出$\{e_1,d_1\}$与$\{e_2,d_2\}$满足

$$e_1d_1\equiv1(\mathrm{mod}\varphi_p(g(x))),1<e_1,d_1<\varphi_p(g(x))$$

$$e_2d_2\equiv1(\mathrm{mod}\varphi_q(g(x))),1<e_2,d_2<\varphi_q(g(x))$$

于是$\{e_1,e_2,g(x),r\}$是公开钥，而$\{d_1,d_2,p,q,\varphi_p(g(x)),\varphi_q(g(x))\}$是秘密钥。

加密算法：设明文 $n=(a_{m-1},a_{m-2},\cdots,a_0)\in\mathbb{Z}_r^m$，计算

$$\langle(a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_0)^{e_1}\rangle_{g(x)}=b_{m-1}^{(1)}x^{m-1}+\cdots+b_1^{(1)}x+b_0^{(1)},$$

$$\langle(a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_0)^{e_2}\rangle_{g(x)}=b_{m-1}^{(2)}x^{m-1}+\cdots+b_1^{(2)}x+b_0^{(2)},$$

这里符号$\langle f(x)\rangle_{g(x)}$表示多项式 $f(x)$模 $g(x)$的余式，其系数模 r。于是

$$(b_{m-1}^{(1)},b_{m-2}^{(1)},\cdots,b_0^{(1)},b_{m-1}^{(2)},b_{m-2}^{(2)},\cdots,b_0^{(2)})\in\mathbb{Z}_r^{2m}$$

作为密文。

解密算法：已知$(b_{m-1}^{(1)},b_{m-2}^{(1)},\cdots,b_0^{(1)},b_{m-1}^{(2)},b_{m-2}^{(2)},\cdots,b_0^{(2)})\in\mathbb{Z}_r^{2m}$，首先计算

$$c_j^{(1)}=\langle b_j^{(1)}\rangle_p,c_j^{(2)}=\langle b_j^{(2)}\rangle_q(j=0,1,\cdots,m-1)。$$

然后分别在$\mathbb{F}_p$与$\mathbb{F}_q$上计算

$$\langle(c_{m-1}^{(1)}x^{m-1}+c_{m-2}^{(1)}x^{m-2}+\cdots+c_0^{(1)})^{d_1}\rangle_{g(x)}=a_{m-1}^{(1)}x^{m-1}+\cdots+a_1^{(1)}x+a_0^{(1)},$$

$$\langle(c_{m-1}^{(2)}x^{m-1}+c_{m-2}^{(2)}x^{m-2}+\cdots+c_0^{(2)})^{d_2}\rangle_{g(x)}=a_{m-1}^{(2)}x^{m-1}+\cdots+a_1^{(2)}x+a_0^{(2)}。$$

对 $j=0,1,\cdots,m-1$，解同余式组

$$\begin{cases}a_j\equiv a_j^{(1)}(\mathrm{mod}p),\\ a_j\equiv a_j^{(2)}(\mathrm{mod}q),\end{cases}$$

因而恢复了明文 $n=(a_{m-1},a_{m-2},\cdots,a_0)\in\mathbb{Z}_r^m$。

解密算法的正确性证明是容易的。

在这个新体制中，如果不能分解大整数 r，则 p,q 未知，因而无法求出 $\varphi_p(g(x))$与 $\varphi_q(g(x))$（即使 $g(x)$的次数 m 取得很小），所以从已知的公开钥不能求出秘密钥。因此，新体制的安全性主要是基于大整数的分解（但是否等价于大整数的分解呢？这是一个没有解决的问题）。此外，新体制也有一个明显的缺限，就是密文具有一些扩展（是明文规模的 2 倍），在密码学中，用密文的扩展换来体制的安全是允许的，也是常用的一种手段。当然，如果能解决 *RSAC*1 中的密文扩展问题，其意义是不言而喻的。我们认为，本文提出的 *RSA* 的新模拟是具有很高安全性的密码体制，它同时还具有易实现的特点。特别是用它们来构造密钥托管和门限密钥托管方案均是方便的。我们期待读者对新体制的有益讨论。

参 考 文 献

1 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Comm ACM, 1978, 21: 120～126

2 Salomaa A. Public-Key Cryptography. New York: Springer-Verlag, 1990

3 曹珍富. 公钥密码学. 哈尔滨: 黑龙江教育出版社, 1993

4 孙琦. 代表整数环上的一类陷门单向函数. 四川大学学报(自然科学版), 1986, (2): 22～27

5 曹珍富. Z[ω]环上的两类密码体制. 电子科学学刊, 1992, 14: 286～290

6 Buchmann J, Willams H C. Quadratic Fields and Cryptography. Number Theory and Cryptography. Loxton J H ed. Cambridge University press, 1990, 9～25

7 孙琦. 关于一类陷门单向函数. 四川大学学报(自然科学版), 1985(4): 33～35

8 Williams H C. Some public-key crypto-functions as intractable as factorization. Cryptologia, 1985, 9: 223～237

9 管纪文. 程序设计基础. 北京: 科学出版社, 1985

(1998-04-22 收到, 1998-12-14 改定)

阅读此文的还阅读了：

26. 关于RSA公钥系统安全性的探讨
27. 关于RSA公钥密码体制安全性问题的探讨
28. RSA加密算法及其安全性研究
29. 基于DES_RSA加密算法的改进与实现
30. 改进RSA算法的安全性分析
31. 公钥密码RSA体制及安全性分析
32. RSA的加密算法与安全性浅析
33. A Novel ASIC Implementation of RSA Algorithm
34. 信息安全和RSA
35. RSA算法安全性分析
36. 提高RSA安全性的几种方法
37. 一种关于CRT-RSA算法的差分错误注入攻击?
38. RSA公钥密码安全性的研究及其FPGA实现
39. RSA与改进的RSA的圆锥曲线模拟
40. 有限域上多项式形式的约化RSA公钥密码算法
41. 基于RSA和Eflash的安全SOC设计
42. 关于 RSA 的模拟
43. RSA的快速实现
44. Factoring RSA modulo N with high bits of p known revisited
45. LLL算法在RSA安全性分析中的应用
46. RSA与背包公钥密码算法的安全性分析
47. RSA密码体制安全性分析
48. RSA算法及其应用
49. 整数分解与RSA的安全性
50. RSA SecurID(r)