Advances in Applied Mathematics 应用数学进展, 2018, 7(11), 1411-1417
Published Online November 2018 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2018.711165

Hans汉斯

Irreducible Polynomials about RSA Type Public Key Cryptosystem over Finite Fields

Binbin Li

School of Mathematical Science, Chang'an University, Xi'an Shaanxi
Email: ytear2828@qq.com

Received: Oct. 23rd, 2018; accepted: Nov. 13th, 2018; published: Nov. 20th, 2018

Abstract

Finite field is one of the most basic mathematical tools of computer science and digital communication field, as well as one of the important branches of modern mathematics. The general theory of finite field mainly starts from the Gauss and Galois, but in recent decades, with the development of discrete mathematics, many mathematicians engaged in applied research and paid attention to the research and application of theory of limited. At the same time, the polynomial theory, especially the properties of irreducible polynomials to analyze various performances of pseudorandom sequence, has a special performance, so the studies of the irreducible polynomials over finite field have been widespreadly concerned in mathematical, coding and cryptology research. This paper found that the PK-RSA simulated security is higher by comparing the irreducible polynomials over finite field to the system of three RSAs.

Keywords

Finite Field, Irreducible Polynomials, RSA Type Public Key Cryptosystem

有限域上的不可约多项式RSA体制

李彬彬

长安大学理学院，陕西 西安
Email: ytear2828@qq.com

收稿日期：2018年10月23日；录用日期：2018年11月13日；发布日期：2018年11月20日

摘 要

有限域是计算科学和数字通讯领域基础的数学工具之一，同时也是现代数学的主要分支之一。有限域的一般理论主要是从Gauss和Galois的工作开始，但最近几十年，随着离散数学的成长与发展，很多专家开

文章引用: 李彬彬. 有限域上的不可约多项式 RSA 体制[J]. 应用数学进展, 2018, 7(11): 1411-1417.
DOI: 10.12677/aam.2018.711165

始慢慢注重有限域理论的研究和应用。同时，多项式理论，特别是不可约多项式的性质对剖析各种伪随机序列的性能有着异常的性能，因此对于有限域上的不可约多项式的研究一直受到数学界、编码与密码领域的广泛关注。尤其是在信息化的时代，人们开始越来越重视自身的信息安全。本文对基于有限域上的不可约多项式对RSA公钥密码体制的三种模拟进行比较，发现PK-RSA模拟安全性更高。

关键词

有限域，不可约多项式，RSA体制

1. 引言

近几十年来，信息安全已经越来越被看作是一种基本的需求，随着安全电子邮件、电子商务和电子政务等各项安全服务日趋增多。随着因特网的普及和通信技术的飞速发展，人们对于信息安全的需求越来越高，而且信息安全和保密信息逐渐成为和人们的生活息息相关的问题。现代密码学是研究保密和通信安全的一门学科，它包括两个方面：一方面是密码编码学，它的主要任务是保护信息，使得信息在传递过程中能够得到很好的保护不被他人窃取、解读和利用，其中用到的主要方法是变换信息；另一方面是密码分析学，它刚好与密码编码学相反，主要任务是如何分析和破译密码，两者之间相互独立又相互促进。公钥密码体制作为信息安全保障框架的基石与技术支撑成为当前信息技术领域中最活跃的因素，人们对这一体制[1] [2] [3]在不同的范畴进行了各种模拟。在 2004 年时，王泽辉和方小洵[4]所写的论文中注释到，确定 $F(p)$ 上的一个 m 次多项式时，构造性算法在技术上是比较复杂的，所以一般会采用概率型算法来解决该问题。目前研究中，较好的算法[2]为：$1/m(m \geq N)$ 需要计算 $p^{m/2}$ 次多项式和 m 次多项式的最小公因式，其中算法的时间复杂度大概就是 $O(p^{m/2})$。然而当对于由低阶构造高阶的解决方案时，就需用到整数的标准分解法。另外，对于确定一个 m 次本原多项式的难度就会更大。对于一大类整数 n (n 为素数乘以素数或 1 的积)，分别给定有限域 $F(p)$ 上 n 次多项式是不可约多项式和本原多项式的一个充要条件[5]，这个条件可以通过 $O(n^3)$ 次 $F(p)$ 上乘法对其进行验证，且易于硬件实现。2009 年，王鑫和王新梅[6]等人在研究论文中提出了一个判断有限域上任意一个多项式是否为不可约多项式、本原多项式的高效确定算法，给出有限域上任意 n 次的多项式是否是不可约和本原多项式的一个充要条件，并通过利用 Euclid 算法，这个判定只需要做 $O((\log_2 n)n^3)$ 次域上乘法，时间比较短，而且容易对硬件的实现。他们[7]提出的算法得到了非常大的提升，并且在验证过程中的适用性得打了更加广泛的应用。

其他的一些判定算法大多都出现在需要使用有限域上[8] [9] [10]，并没有针对改进算法或高效算法判定有限域上多项式不可约性和本原性提出，本文在这儿也不对其再做陈述。下面本文将对有限域上不可约多项式的 RSA 的模拟进行论述。

2. 基于有限域上不可约多项式的 RSA 的模拟一

2.1. 密钥生成

1) 假设 p 和 q 都是大素数，且满足 $p<q, r=pq$，选择 F_p 上的一个首项系数为 1 的 m 次多项式为 $g(x)$，使其在 F_p 上满足分解式 $g(x)=g_1^{(1)}(x)g_2^{(1)}(x)\cdots g_{k_1}^{(1)}(x)$，其中 $g_i^{(1)}(x)$ 为 F_p 上的 $m_i^{(1)}$ 次不可约多项式

$(i=1,2,\cdots,k_1)$，同时 $g(x)$ 在 F_q 上满足分解式：

$g(x)=g_1^{(2)}(x)g_2^{(2)}(x)\cdots g_{k_2}^{(2)}(x)$，$g_i^{(2)}(x)$ 为 F_q 上的 $m_i^{(2)}$ 次不可约多项式 $(i=1,2,\cdots,k_2)$；

2) 根据欧拉函数的通式易得：

$$\phi_p(g(x))=p^m\prod_{i=1}^{k_1}\left(1-\frac{1}{p^{m_i^{(1)}}}\right),\quad \phi_q(g(x))=q^m\prod_{i=1}^{k_2}\left(1-\frac{1}{p^{m_i^{(2)}}}\right);$$

3) 根据 Euclid 算法：$e_1d_1\equiv 1\bmod\left(\phi_p(g(x))\right),1<e_1,d_1<\phi_p(g(x))$，得：

$$e_2d_2\equiv 1\bmod\left(\phi_q(g(x))\right),1<e_2,d_2<\phi_q(g(x))$$

则可求得：$\{e_1,d_1\}$ 和 $\{e_2,d_2\}$；

4) 可计算得其公钥为：$\{e_1,e_2,g(x),r\}$，私钥为：$\{d_1,d_2,p,q,\phi_p(g(x)),\phi_q(g(x))\}$。

2.2. 加密算法

假设明文为 $(a_{m-1},a_{m-2},\cdots,a_1,a_0)\in Z_r^m$；则计算得：

$$\left\langle\left(a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1+a_0\right)^{e_1}\right\rangle_{g(x)}=b_{m-1}^{(1)}x^{m-1}+b_{m-2}^{(1)}x^{m-2}+\cdots+b_1^{(1)}x+b_0^{(1)};$$

$$\left\langle\left(a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0\right)^{e_2}\right\rangle_{g(x)}=b_{m-1}^{(2)}x^{m-1}+b_{m-2}^{(2)}x^{m-2}+\cdots+b_1^{(2)}x+b_0^{(2)};$$

其中 $\langle f(x)\rangle_{g(x)}$ 表示不可约多项式 $f(x)$ 模 $g(x)$ 的余式，系数模 r，则可将：

$$\left(b_{m-1}^{(1)},b_{m-2}^{(1)},\cdots,b_1^{(1)},b_0^{(1)};b_{m-1}^{(2)},b_{m-2}^{(2)},\cdots,b_1^{(2)},b_0^{(2)}\right)\in Z_r^{2m}$$ 作为密文。

2.3. 解密算法

1) 已知 $(b_{m-1},b_{m-2},\cdots,b_1,b_0)\in Z_r^m$，可得：

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

2) 在 F_p 和 F_q 上分别计算：

$$\left\langle\left(c_{m-1}^{(1)}x^{m-1}+c_{m-2}^{(1)}x^{m-2}+\cdots+c_1^{(1)}x+c_0^{(1)}\right)^{d_1}\right\rangle_{g(x)}=a_{m-1}^{(1)}x^{m-1}+a_{m-2}^{(1)}x^{m-2}+\cdots+a_1^{(1)}x+a_0^{(1)};$$

$$\left\langle\left(c_{m-1}^{(1)}x^{m-1}+c_{m-2}^{(1)}x^{m-2}+\cdots+c_1^{(2)}x+c_0^{(2)}\right)^{d_2}\right\rangle_{g(x)}=a_{m-1}^{(2)}x^{m-1}+a_{m-2}^{(1)}x^{m-2}+\cdots+a_1^{(2)}x+a_0^{(2)}。$$

3) 解同余方程组：

$$\begin{cases}a_j\equiv a_j^{(1)}\bmod p\\ a_j\equiv a_j^{(2)}\bmod q\end{cases}(j=0,1,2,\cdots,m-1)$$

则明文为 $(a_{m-1},a_{m-2},\cdots,a_1,a_0)\in Z_r^m$。

2.4. 算法分析

由于分解有限域 F_p 上的 m 次不可约多项式的时间复杂程度为 $O(pm^3)$。所以，当 p 过小时，有限域上分解的时间复杂度仅为 $O(m^3)$，则仍为多项式形式的复杂度，那么该体制是不安全的。而当 p 过大时，

Berlekamp 算法就对分解就没有意义，且此时限制多项式 $g(x)$ 的次数不能过大，更不必讨论对于多项式的加密和解密了。假设 $g(x)$ 次数不够大，由于 $g(x)$ 公开，人们将会利用列举法对 $g_i(x)$ 的次数进行破解易将密码体制破解，造成信息的泄露。所以这种算法是不安全的。

3. 基于有限域上不可约多项式的 RSA 的模拟二

3.1. 密钥生成

1) 假设 p 和 q 都是大素数，并且满足 $p<q, r=pq$，选择 F_p 上的一个首项系数是 1 的 m 次多项式是 $g(x)$，使得它在 F_p 上满足分解式 $g(x)=g_1^{(1)}(x)g_2^{(1)}(x)\cdots g_{k_1}^{(1)}(x)$，其中的 $g_i^{(1)}(x)$ 分别是 F_p 上的 $m_i^{(1)}$ 次不可约多项式 $(i=1,2,\cdots,k_1)$，同时使得 $g(x)$ 在 F_q 上满足分解式 $g(x)=g_1^{(2)}(x)g_2^{(2)}(x)\cdots g_{k_2}^{(2)}(x)$，$g_i^{(2)}(x)$ 分别是 F_q 上的 $m_i^{(2)}$ 次不可约多项式 $(i=1,2,\cdots,k_2)$；

2) 计算 $\phi_r(g(x))=\phi_p(g(x))\phi_q(g(x))=r^m\prod_{i=1}^{k_1}\left(1-\frac{1}{p^{m_i^{(1)}}}\right)\prod_{i=1}^{k_2}\left(1-\frac{1}{p^{m_i^{(2)}}}\right)$；

3) 根据 Eulid 算法：$ed\equiv 1\bmod\left(\phi_r(g(x))\right), 1<e,d<\phi_r(g(x)), \gcd\left(e,\phi_r(g(x))\right)=1$，
那么就会有明文空间和密文空间都是 Z_r^m；其中的 $p,q,\phi_p(g(x)),\phi_q(g(x))$ 是保密的；

4) 那么会有公钥是 $\{e,r,g(x)\}$，私钥是 $\{d,g(x)\}$。

3.2. 加密算法

假设明文 $(a_{m-1},a_{m-2},\cdots,a_1,a_0)\in Z_r^m$，计算：

$$\left\langle\left(a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+ax+a_0\right)^e\right\rangle_{g(x)}=b_{m-1}x^{m-1}+b_{m-2}x^{m-2}+\cdots+b_1x+b_0;$$

其中的 $\langle f(x)\rangle_{g(x)}$ 表示的是多项式 $f(x)$ 模 $g(x)$ 的余式，系数模 r，那么可将：

$$(b_{m-1},b_{m-2},\cdots,b_1,b_0)\text{ 作为密文。}$$

3.3. 解密算法

1) 已知 $(b_{m-1},b_{m-2},\cdots,b_1,b_0)\in Z_r^m$，计算：

$$\left\langle\left(b_{m-1}x^{m-1}+b_{m-2}x^{m-2}+\cdots+b_1x+b_0\right)^d\right\rangle_{g(x)}=a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0,$$

2) 求出明文：

$$(a_{m-1},a_{m-2},\cdots,a_1,a_0)\in Z_r^m\text{。}$$

3.4. 算法分析

因为在算法中 p 和 q 都是比较大的素数，所以 $\phi_r(g(x))$ 也是比较大的数，它会导致 e,d 也比较大，从而导致在应用中加密和解密速度滞后，所以也是不太可取的。

在分析了上面有限域上不可约多项式的 RSA 的两种模拟后发现对公钥密码体制的解密和加密都是不可取的，在各方面都存在安全隐患，针对这一问题，对一种新的算法进行表述并对其进行了实例验证。

4. 基于不可约多项式的 PK-RSA 公钥密码算法

在设计算法之前，在这儿先给出其中要用到的两个定义，第一个是拟明文：将所有形式的明文数字都转化成 0、1 序列后，异或一个 0、1 序列得到的序列就成为拟明文。例如，明文数字化后的序列是 $(1,0)$，

选择异或的序列是$(0,1)$，那么可以得到拟明文序列是$(1,0)\oplus(0,1)=(1,1)$。第二个是相伴多项式：在F_p有限域上，任意多项式都可以化为首项系数是 1，其余的各项系数都是正数的相伴多项式。例如，多项式$(-2x^2-1)$经过一系列变换，$(-2x^2-1)\to 3*(-2x^2-1)\to(-6x^2-3)\to(x^2+4)$，就变成了有限域$F_7$上的相伴多项式为$(x^2+4)$。

4.1. 密钥生成

1) 假设p和q都是大素数，并且其能够满足$p<q, r=pq$，选择F_p上的一个首项系数是 1 的m次多项式为$g(x)$，使其在F_p上满足分解式$g(x)=g_1^{(1)}(x)g_2^{(1)}(x)\cdots g_{k_1}^{(1)}(x)$，其中的$g_i^{(1)}(x)$是$F_p$上的$m_i^{(1)}$次不可约多项式$(i=1,2,\cdots,k_1)$，同时$g(x)$在$F_q$上满足分解式$g(x)=g_1^{(2)}(x)g_2^{(2)}(x)\cdots g_{k_2}^{(2)}(x)$，$g_i^{(2)}(x)$为$F_q$上的$m_i^{(2)}$次不可约多项式$(i=1,2,\cdots,k_2)$；

2) 计算$\phi_r(g(x))=\phi_p(g_p(x))\phi_q(g_q(x))=r^m\prod_{i=1}^{k_1}\left(1-\frac{1}{p^{m_i^{(1)}}}\right)\prod_{i=1}^{k_2}\left(1-\frac{1}{p^{m_i^{(2)}}}\right)$和$\phi_p(g_p(x))=r^m\prod_{i=1}^{k_1}\left(1-\frac{1}{p^{m_i^{(1)}}}\right)$；

3) 恰当的因子，则$\phi_p(g_p(x))$的一个大因子是k；

4) 在有限域F_p上计算方程$x^k\equiv 1(\bmod g_p(x))$的$k$次本原根$h(x)$，并且满足$h(x)\in F_p[x]$，$h(x)$的全体解记作$S_p^k(g(x))$；

5) 选择一个和k互素的e，并且有$(e>1)$；

6) 计算d，使得它满足$ed\equiv 1(\bmod k)$，那么公钥$(e,r,g(x))$，私钥$(d,r,g(x))$；

7) 严格的保密p,q,k，使得它不能被销毁，为的是系统能够继续利用。

4.2. 加密算法

1) 将计算明文m数字化成 0、1 序列，根据解空间$S_p^k(g(x))$中的某个特定解$h(x)$经一个异或序列$r(x)$，将明文序列$m(x)$异或此序列得到一个拟明文序列$m'(x)$，即满足$m(x)\oplus r(x)=m'(x)$；

2) 计算明文$\langle m'(x)^e\rangle_{g(x)}=c(x)$，其中的$\langle f(x)\rangle_{g(x)}$表示多项式$f(x)$模$g(x)$的余式，系数模$p$，那么将$c(x)$作为密文。

4.3. 解密算法

已知$c(x)\in S_p^k(g(x))$，

1) 计算拟明文：$\langle c(x)^d\rangle_{g(x)}=m'(x)$，并且$m'(x)\in S_p^k(g(x))$；

2) 恢复明文：$m'(x)\oplus r(x)=m(x)$。

4.4. 算法分析

首先，改算法保证了p,q,e,d,k和$g(x)$具有一定的数量级。其次，在选取的$g(x)$在F_p和F_q上的分解式也是可行的。另外，多项式的乘幂运算实际上就将是不可约多项式相乘，就是求有限域F_p上的序列卷积，它可用快速数论变换来实现。在此基础上，可通过计算机程序来求解$x^k\equiv 1(\bmod g(x))$的k次本原根$h(x)$，即将有限域F_p上所有的不可约多项式代入方程进行求模，$h(x)$的最高次可以取$0\to m-1$，每项的系数可以取$0\to p-1$，即可得出解空间的计算是非常容易的。PK-RSA 算法的每一步都是可行的，而且计算量和保密度都优于前面两种 RSA 新模拟。下面对 PK-RSA 新公钥体制的实例进行验证。

4.5. 算法验证

1) 密钥的生成

a) 首先，选择两个保密的大素数比如 $p=7,q=5,rq=35$，接下来选择一个多项式是 $g(x)=x^4+2x^2+1$，那么根据多项式分解定理，一方面可 $g(x)=x^4+2x^2+1$ 分解成为 $g_7(x)=(x^2+1)^2$，使得 (x^2+1) 成为 $F_7(x)$ 上的 2 次不可约多项式，另一方面可将 $g(x)=x^4+2x^2+1$ 分解成 $g_5(x)=(x+2)^2(x+3)^2$，使得 $(x+2),(x+3)$ 为 $F_5(x)$ 中的一次不可约多项式。

b) 然后计算：$\phi_{35}(g(x))=\phi_7\left((x^2+1)^2\right)\phi_5\left((x+2)^2(x+3)^2\right)=35^4\left(1-\frac{1}{7^2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{5}\right)$，进而有：

$$\phi_{35}(g(x))=940800=2352\times400=\left(2^4\times3\times7^2\right)\times\left(2^4\times5^2\right)=3\times2^8\times5^2\times7^2。$$

c) 选择 $\phi_7(g_7(x))$ 中的一个恰当的大因子为 7。

d) 计算方程 $x^7\equiv1\left(\mathrm{mod}\left((x^2+1)^2\right)\right)$ 的 7 次本原根 $h(x)$，因为 7 为 $\phi_7(g_7(x))$ 的因子，那么根据模理论可知，模 $g_7(x)$ 的 7 次本原根 $h(x)$ 就一定存在，而且其中的一个是 x^2+2，并且它的解空间是 $(x^2+2)^4,(x^2+2)^5,(x^2+2)^6$，可知这些都为 $S_7^7\left((x^2+1)^2\right)$ 中的元素，除了这些可能还有其他元素，其中的 $(x^2+2)^0=1$ 是平凡的本原根。

e) 选择一个和 7 互素的 e，令 $e=2$。

f) 计算 d，满足 $2d\equiv1\bmod7$ (因为 2 和 7 互素，其中的 d 一定存在，并且有 $d=4$，那么就有拟明文和密文空间都是 $S_7^7\left((x^2+1)^2\right)$。

g) 于是公钥是 $(2,35,x^4+2x^2+1)$，私钥是 $(4,35,x^4+2x^2+1)$。

h) 要求严格的保密 7、5、7，但是不能销毁。

2) 加密算法

a) 将任意明文 m 数字化成 0、1 序列 $(1,1,1,0)$；

b) 根据解空间中的某个特定解 $h(x)=(1,0,10)$，经一个异或序列 $r(x)=(0,1,00)$，将明文序列 $m(x)=(1,1,10)$ (在这儿根据 $h(x)$ 的形式已经将任意明文进行了分段，使得明文和 $h(x)$ 的形式相同)异或者次序列得到一个拟明文序列 $m'(x)=(1,0,10)$，并且 $(1,0,10)\in S_7^7\left((x^2+1)^2\right)$ (其中的拟明文不是真正明文，而是被适当异或的明文)，即计算 $m(x)\oplus r(x)=m'(x)$，可得 $(1,1,10)\oplus(0,1,00)=(1,0,10)$。

c) 计算密文 $\left\langle(x^2+2)^2\right\rangle_{(x^2+1)^2}=x^2+5$，并选择 $S_7^7\left((x^2+1)^2\right)$ 中的一个元素 x^2+2 作为拟明文 $m'(x)$，那么就有 $m'(x)=(1,0,2)$，进行下面的加密操作 $\left\langle(x^2+2)^2\right\rangle_{(x^2+1)^2}=x^2+5$，这里 $\left\langle(x^2+2)^2\right\rangle_{(x^2+1)^2}$ 表示多项式 $(x^2+2)^2$ 模 $(x^2+1)^2$ 的余式，系数模为 7。于是可以将 $(1,0,5)$ 作为密文。

3) 解密算法

已知 $(1,0,5)\in S_7^7\left((x^2+1)^2\right)$

a) 计算 $\left\langle(x^2+5)^4\right\rangle_{(x^2+1)^2}=x^2+2$，这样就得到了拟明文 $(1,0,2)\in S_7^7\left((x^2+1)^2\right)$。

b) 恢复明文：$m'(x)\oplus r(x)=m(x)$，即得 $(1,0,10)\oplus(0,1,00)=(1,1,10)$。

致　谢

感谢我的导师郑素佩老师对于我的指导。

参考文献

[1] 张青坡, 陈彩云, 陈鲁生, 陈艳玲. 有限域上多项式形式的 ElGamal 体制及数字签名方案[J]. 通信学报, 2005, 26(5): 69-72.

[2] 张斌, 白恩健, 肖国镇. 关于 RSA 的模拟[J]. 西安电子科技大学学报(自然科学版), 2002, 29(4): 518-521.

[3] 李雅峰. 有限域上多项式形式的约化 RSA 公钥密码算法[D]: [硕士学位论文]. 昆明: 云南大学, 2012.

[4] 王泽辉, 方小洵. F_p 上不可约与本原多项式的高效确定算法[J]. 中山大学学报(自然科学版), 2004, 43(6): 89-92.

[5] 田力, 张宗明. 有限域上的方程与不可约多项式[J]. 泰山学院学报, 2011, 33(6): 4-6.

[6] 王鑫, 王新梅, 韦宝典. 判定有限域上不可约多项式及本原多项式的一种高效算法[J]. 中山大学学报(自然科学版), 2009, 48(1): 6-9.

[7] 何丽. 有限域上的多项式及其在公钥密码体制中的应用[D]: [硕士学位论文]. 大连: 辽宁师范大学, 2008.

[8] 赵正俊. 有限域上的不可约多项式及其分布[D]: [硕士学位论文]. 南京: 南京航空航天大学, 2009.

[9] 张宗明. 有限域上的不可约多项式的存在性与求法[J]. 开封大学学报, 1993, 141(3): 38-41.

[10] 张宗明. P^k 元域中元素的 n 次根[J]. 周口师范学院学报, 2011, 33(2): 16-19.