高效的原根生成算法

夏静波　张四兰　陈建华
(武汉大学数学与统计学院,武汉 430072)
E-mail:kaleshouse@163.com

摘　要　在研究一般的原根生成算法的基础上,提出了一种不依赖于广义黎曼猜想的概率性多项式时间算法,该算法能够以指定的概率确保输出正确。根据算法复杂度的分析,该算法为多项式时间算法,易于实现。

关键词　原根　次数　ERH

文章编号 1002-8331-(2006)11-0032-03　**文献标识码** A　**中图分类号** TP309

Effective Algorithm for Primitive Roots Generation

Xia Jingbo　Zhang Silan　Chen Jianhua
(School of Mathematics and Statistics, Wuhan University, Wuhan 430072)

Abstract: By analysing the generation algorithm of primitive root, we put forward a probabilistic algorithm, in which the error probability of this algorithm can be totally controlled. Our algorithm is with polynimial time complexity, and it is easy to implementation.

Keywords: primitive root, order, ERH

1　引言

原根的应用在信息安全领域非常广泛,当今许多密码协议的核心都包括原根的生成,如 Diffie-Hellman 密钥交换和 Elgamal 签名协议;一些密码机制,如椭圆曲线密码中阶的计算也需要原根。早在上个世纪 50 年代王元院士[1]就证明了模 p 的最小原根(记为 $g(p)$)有如下结果:$g(p)=O(p^{\frac{1}{4}+\varepsilon})$,在 ERH(广义 Riemann 猜想)下,$g(p)=O(m^6\log^2 p)$,其中 m 为 $p-1$ 的不同素因子个数。1992 年,Victor Shoup[2]改进了王元的结果,在 ERH 下得到 $g(p)=O(\log^6 p)$,构造了含原根的小集合 S,并给出了确定的多项式算法。Johannes Buchmann 和 Victor Shoup[3]将模 p 推广到模 p^n。之后,Eric Bach[4]将 $p-1$ 部分分解,也给出了依赖于 ERH 的多项式时间算法。本文分析研究了 Eric Bach 算法,将其改进为不依赖于 ERH 的多项式时间概率算法,该算法能够以指定的正确概率输出原根。

2　基础知识

定义 1　若 $m>1,(a,m)=1$,则使得同余式 $a^\gamma\equiv 1(\mathrm{mod}\ m)$ 成立的最小正整数 γ 叫作 a 模 m 的次数;当 $\gamma=p-1$ 时,我们称 a 为模 m 的原根。

在这里,我们列出四个有用的定理。

定理 1　m 有原根存在的充要条件为 $m=2,4,p^l,2p^l$,其中 p 为奇素数。参考文献[5]。

定理 2　a 模 m 次数为 γ,$a^l\equiv 1(\mathrm{mod}\ m)$,则 $\gamma|l$。参考文献[5]。

定理 3　若 a 模 m 的次数为 γ_1,b 模 m 的次数为 γ_2,且 $(\gamma_1,\gamma_2)=1$,则 ab 模 m 的次数为 $\gamma_1\gamma_2$。参考文献[6]。

定理 4　若 p 为素数,$C>1$,$B\log B=C\log p$,$B\geqslant 1$,则 $\sum_{\substack{q|p-1\\ q>B}}1<\frac{1}{C}$,且有 $B\sim C(\frac{\log p}{\log\log p})$,$\pi(B)\sim C\frac{\log p}{(\log\log p)^2}$。参考文献[4]。

本文主要讨论 $m=p$ 时的原根问题。

3　依赖于 ERH 的多项式时间原根生成算法

生成模 p 原根最原始的思想就是:通过逐个计算 $g^i(i=1,2,\cdots,p-1)$,求出 g 的次数,由此判断 g 是否为原根,这显然是指数算法,实现效率非常低;经典的加速方法将 $p-1$ 完全分解为 $q_1^{e_1}\cdots q_\omega^{e_\omega}$,通过计算 $g^{\frac{p-1}{q_i}}\equiv 1(\mathrm{mod}\ p)$ 是否成立来生成原根,这个算法似乎能够提高效率,可糟糕的是大整数的分解没有多项式算法。1997 年,Eric Bach 利用部分分解的思想给出了依赖于 ERH 的确定的多项式时间算法。

算法 1

输入:素数 $p\geqslant 3$。

输出:含原根的小集合 S。

Step1　计算 B,满足 $B\log B=30\log p$

Step2　分解 $p-1=q_1^{e_1}\cdots q_\omega^{e_\omega}Q$,其中 $q_i<B$,Q 与小于 B 的素数互素。

Step3　for $i=1$ to ω

随机选择素数 $b_i\leqslant 2(\log p)^2$,$b_i^{\frac{p-1}{q_i}}\neq 1(\mathrm{mod}\ p)$,

$a_i\equiv b_i^{\frac{p-1}{q_i^{e_i}}}(\mathrm{mod}\ p)$,令 $a=\prod_{i=1}^{\omega}a_i$

Step4　构造集合 S 为

基金项目:国家 863 高技术研究发展计划资助项目(编号:2001AA141010)

作者简介:夏静波(1979-),博士研究生,主要研究方向:数论与密码学、不定方程。张四兰(1980-),硕士研究生,主要研究方向:数论与密码学、信息安全。陈建华(1963-),教授,博士生导师,主要研究方向:密码学、数论、信息安全、芯片设计。

$$S=\left\{ab^{\frac{p-1}{Q}}(\bmod p);b\leqslant 5\frac{(\log p)^4}{(\log\log p)^2},b\text{ 为素数}\right\}$$

输出 S,结束

根据 ERH,满足算法要求的 b_i 与 b 能够被取到,从而保证集合 S 一定含有模 p 原根。参考文献[4]。

算法 1 的主要运算是 a 的构造和集合 S 的生成。由定理 4 知 $\omega=O(\frac{\log p}{(\log\log p)^2})$;又由素数定理(参考文献[7])$\pi(x)\sim\frac{x}{\log x}$ 知寻找 b_i 的最坏情况要进行 $O\left(\frac{(\log p)^2}{\log\log p}\right)$ 次模幂运算,其中每次模幂运算需要 $O(\log p)$ 次模乘,一次模乘需要 $O(\log p)^2$ 次位操作(若采用快速乘法只需要 $O(\log p)^{1+\varepsilon}$ 个位操作($0<\varepsilon<1$)),则构造 a 的时间复杂度为 $O\left(\frac{(\log p)^6}{(\log\log p)^3}\right)$。根据同样的分析,生成 S 集合需要 $O\left(\frac{(\log p)^7}{(\log\log p)^3}\right)$ 次位操作,若采用快速算法可将复杂度降为 $O\left(\frac{(\log p)^6}{(\log\log p)^{2+O(1)}}\right)$。算法 1 作为多项式算法有它的可行性,但依赖于 ERH 导致在实际应用中得不到实施。进一步,将其改进为不依赖 ERH 的多项式时间概率算法。

4 不依赖于 ERH 的高效原根生成算法

在实际应用中,生成原根的确定性算法不仅理论比较艰深,并且在计算中实现复杂,由操作误差、实现复杂性带来的不正确安全隐患要比概率性算法带来的误差大得多,况且概率性算法的误差可以被控制在一个极小的范围内,如$\left(\frac{1}{2}\right)^{40}$。这样的误差可以完全被接受。基于此,将算法 1 改进为概率性算法。

算法 2

输入:素数 $p\geqslant 3$,错误概率 ε,$0<\varepsilon<1$。

输出:输出原根 g,且正确概率不小于 $1-\varepsilon$。

Step1 计算 B,满足$(1+\frac{p-1}{2})(1-\frac{1}{B})^{\log_B\frac{p-1}{2}}=1-\varepsilon$

Step2 部分分解 $p-1=q_1^{e_1}\cdots q_\omega^{e_\omega}Q$

Step3 for $i=1$ to ω

随机选择 a_i,$a_i^{\frac{p-1}{q_i}}\neq 1(\bmod p)$

计算 $a=\prod_{i=1}^{\omega}a_i^{\frac{p-1}{q_i^{e_i}}}(\bmod p)$

Step4 If Q 为素数,then 以确定性的结果输出 a,结束

else 随机选择 b,若满足 $b^{\frac{p-1}{Q}}\neq 1(\bmod p)$,就返回 $g=ab^{\frac{p-1}{Q}}$,

正确概率为$(1+\frac{1}{Q-1})(1-\frac{1}{B})^{\log_B Q}$,结束

该算法将算法 1 中构造含原根的集合 S 的方法进行改进,转变为寻找一个次数可能为 Q 的元素 $b^{\frac{p-1}{Q}}$,其可能性大于 $1-\varepsilon$,从而输出为原根的概率不会小于 $1-\varepsilon$。具体证明见以下定理。

定理 5 算法 2 输出为原根的概率不小于 $1-\varepsilon$。

在证明定理之前先证明以下 4 个引理(引理中所出现的符号与算法 2 中规定的一致):

引理 1 $A=\left\{b^{\frac{p-1}{Q}},b\in Z/pZ^*,b^{\frac{p-1}{Q}}\text{ 次数为 }Q\right\}$,则 A 所含元素个数 $\#A=\varphi(Q)$,其 φ 为 Euler 函数。

证明:设 x 模 p 的次数 Q,g 为模 p 的一个原根,x 关于 g 的指数 $Ind_g^x=m$,$x^Q\equiv 1(\bmod p)$,则 $g^{mQ}\equiv 1(\bmod p)$,因此 $p-1|mQ$,即 $\frac{p-1}{Q}|m$,$m=\mu(\frac{p-1}{Q})$,$x\equiv g^m\equiv g^{\mu(\frac{p-1}{Q})}(\bmod p)$,令 $b=g^\mu$,则 $x=b^{\frac{p-1}{Q}}$。而模 p 缩余系中所有次数为 Q 的元素有 $\varphi(Q)$ 个,故 $\#A=\varphi(Q)$。

引理 2 有 $\frac{p-1}{Q}$ 个模 p 不同的 b_i,使得 $ab_i^{\frac{p-1}{Q}}$ 生成同一个原根 g,不同原根由不同 b_i 生成。

证明:a 次数为 $\frac{p-1}{Q}$,引理 1 确保存在 v 使得 $a=g^{vQ}$,设 b 指数为 $Ind_g^b=m_1$,则 $g\equiv ab^{\frac{p-1}{Q}}\equiv g^{vQ+m_1}(\bmod p)vQ+m_1\equiv 1(\bmod p-1)$,$m_1\equiv m_0\ (\bmod\ Q)$,$0\leqslant m_0<Q$,$b_i=g^{m_0+iQ}$,$0\leqslant i\leqslant(\frac{p-1}{Q})-1$,$g\equiv ab_i^{\frac{p-1}{Q}}\equiv ab_j^{\frac{p-1}{Q}}(\bmod p)$,故有 $\frac{p-1}{Q}$ 个模 p 不同的 b_i,使得 $ab_i^{\frac{p-1}{Q}}$ 生成同一个原根 g,不同原根由不同 b_i 生成。

引理 3 方程 $b^k\equiv 1(\bmod p)$ 解个数恰好为 k。

证明:因为次数为 d(其中 $d|p-1$)的元素有 $\varphi(d)$ 个,所以方程解数为 $\sum_{d|k}\varphi(d)=k$。

引理 4 证明 $\frac{\varphi(Q)}{Q-1}>1-\varepsilon$。

证明:设 $\omega(Q)$ 为 Q 的不同素因子个数,$\omega(Q)\leqslant\log_8 Q$[8]。完全分解 Q,$Q=\prod_{i=1}^{\omega(Q)}p_i^{t_i}$,$\varphi$ 为积性函数,且 $p_i>B$,则:

$$\frac{\varphi(Q)}{Q-1}=\frac{Q\prod_{i=1}^{\omega(Q)}(1-\frac{1}{p_i})}{Q-1}=(1+\frac{1}{Q-1})\prod_{i=1}^{\omega(Q)}(1-\frac{1}{p_i})>$$

$$(1+\frac{1}{Q-1})\prod_{i=1}^{\omega(Q)}(1-\frac{1}{B})=(1+\frac{1}{Q-1})(1-\frac{1}{B})^{\omega(Q)}>$$

$$(1+\frac{1}{Q-1})(1-\frac{1}{B})^{\log_8 Q}>1-\varepsilon$$

现在利用以上引理,给出定理 5 的证明:

证明:引理 1,引理 2 证明了有 $\frac{p-1}{Q}\varphi(Q)$ 个 b 使得 $g=ab^{\frac{p-1}{Q}}$ 是原根。而由引理 3 知,Step4 中满足 $b^{\frac{p-1}{Q}}\neq 1(\bmod p)$ 的 b 有 $p-1-\frac{p-1}{Q}$ 个,所以算法 2 中输出的 g 是原根的概率为:

$$\frac{\frac{p-1}{Q}\varphi(Q)}{p-1-\frac{p-1}{Q}}=\frac{\varphi(Q)}{Q-1}>1-\varepsilon$$

下面我们来分析算法的计算复杂度。

由于整个算法中比较耗时的就是分解与模幂运算,其中分解使用 Pollard'rho 方法所需要的平均位操作数为 $O(\sqrt{B}(\log p)^2)$;由 $\omega(p-1)$ 平均大小为 $O(\log\log p)$ 知,整个算法所要

进行的模幂运算次数为 $O(\log\log p)$。与算法 1 的分析类似，算法 2 的复杂度为 $O(\sqrt{B}\ (\log p)^2+(\log p)^3\log\log p)$，这里 $B<\frac{1}{\varepsilon}$，故算法复杂度为 $O(\sqrt{\frac{1}{\varepsilon}}\ (\log p)^2+(\log p)^3\log\log p)$。

需要注意的是，复杂度里含有非多项式因子 $\frac{1}{\varepsilon}$，导致算法 2 难以实施，因此算法实现的最关键问题就是消去非多项式因子。

为了消去非多项式因子，我们做了各种尝试。

一种有意义的尝试是把算法 2 中的 B 减小到 $O(\log p)^\alpha$，如 $B\leqslant(\log p)^2(\log\log p)$，就可以消去非多项式因子，这时算法的复杂度为 $O((\log p)^3\log\log p)$。但仍然存在着一个问题，就是当 p 比较小的时候，虽然实验表明此算法的正确性很高，一般不会低于 $1-\left(\frac{1}{2}\right)^{40}$（甚至 $B=2^{40}$），但理论上的正确概率并不能保障。尽管如此，在对正确概率要求不是特别高的情况下，这种改进后的算法依然可以使用，并且速度非常快。

这个改进在理论证明上存在缺陷。为了从理论上保障原根输出的概率，我们给出另外一个改进算法，该算法不但可以消去非多项式因子，而且严格保证输出的正确概率大于某一固定值，如 $1-\left(\frac{1}{2}\right)^{40}$，其主要思想是在 p 比较小的情况下完全分解 $p-1$，具体算法为：

算法 3

输入：素数 $p\geqslant 3$。

输出：模 p 原根，且正确概率不小于 $1-\left(\frac{1}{2}\right)^{40}$。

Step1 If $p<2^{30}$ then goto Step2

else goto Step3

Step2 完全分解 $p-1$，用算法 2 输出原根，此时为确定性算法，结束

Step3 $B=(\log p)^{5.090\,920}$，用算法 2 输出原根 g，且正确概率不小于 $1-\left(\frac{1}{2}\right)^{40}$，结束

用算法 2 的分析方法，可得此算法的复杂度为：$O(\sqrt{B}\ (\log p)^2+(\log p)^3\log\log p)$，即 $O(\sqrt{(\log p)^{5.090\,920}}\ (\log p)^2+(\log p)^3\log\log p)=O(\log p)^{4.954\,960}$，这样就消去了非多项式因子。又由 $(1+\frac{1}{Q-1})(1-\frac{1}{B})^{\log_g Q}>1-\left(\frac{1}{2}\right)^{40}$ $(p>2^{30})$ 知输出为原根的概率不会小于 $1-\left(\frac{1}{2}\right)^{40}$。若完全分解更大的 $p-1$，同时适当调整 B 的大小，正确概率就会进一步提高。

相对于前两个算法，算法 3 速度快，正确概率大，是一个易于实施的算法。现将文章中的三种算法的复杂度、概率等进行比较，具体数据见表 1。

表 1　三种不同算法的比较

	复杂度	算法分析	是否依赖于 ERH	正确概率
算法 1	$O(\frac{(\log p)^7}{(\log\log p)^3})$	确定性算法	是	1
算法 2	$O(\sqrt{\frac{1}{\varepsilon}}\ (\log p)^2+(\log p)^3\log\log p)$	概率性算法	否	大于 $1-\varepsilon(0<\varepsilon<1)$
算法 3	$O(\log p)^{4.954\,960}$	概率性算法	否	大于 $1-\left(\frac{1}{2}\right)^{40}$

5　结束语

我们从研究原根入手，分析了 Eric Bach 提出的原根生成算法，指出其对 ERH 的依赖性。紧接着将其改进为不依赖于 ERH 的新的算法，为了提高这种算法的可实施性，通过各种研究，最终提出一种概率性的多项式时间算法。实验表明，该算法不但可以以指定的正确概率输出原根，而且易于实现。

（收稿日期：2005 年 12 月）

参考文献

1.王元.论素数的最小正原根[J].数学学报，1959；(9)：432~441

2.Victor Shoup.Searching for primitive roots in finite fields[J].Mathematics of Computation，1992；58：369~380

3.Johannes Buchmann，Victor Shoup.Constructing nonresidues in finite fields and the extended Riemann hypothesis[J].Mathematic of Computation，1996；65：1311~1326

4.Eric Bach.Comments on search procedures for primitive roots[J].Mathematics of Computation，1997；66：1719~1724

5.华罗庚.数论导引[M].科学出版社，1957

6.张禾瑞.近世代数[M].高等教育出版社，1978

7.冯克勤.代数数论[M].科学出版社，2001

8.Guy Robin.Estimation de la fonction de tchebycheff θ sur le k-ieme nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n[J].Acta Arithmetica，2003；62：367~389

（上接 31 页）

算中出现的问题及其根本原因。提出了一种新的规则分辨矩阵，该分辨矩阵在存储空间、计算量方面优于原对象分辨矩阵。阐述了其在求信息论观点下的属性核与约简簇，度量约简造成的决策信息系统不确定性的变化，以及比较同一决策信息系统不同约简的不确定性程度几方面的应用。

（收稿日期：2005 年 12 月）

参考文献

1.Pawlak Z.Rough Sets：Theoretical Aspects of Reasoning About Data[M].Dordrecht：Kluwer Academic Publishers，1991

2.Hu XiaoHua，Cercone N.Learning in relational databases：a rough set approach[J].Computational Intelligence，1995；11(2)：323~337

3.叶东毅，陈昭炯.一个新的差别矩阵及其求核方法[J].电子学报，2002；30(7)：1086~1088

4.Mollestad T，Skowron A.A rough set framework for datamining of prepositional default rules[C].In：Proc of 9th International Symposiumon Foundations of Intelligent Syetems，ISMIS，1996；448~457

5.王国胤.决策表核属性的计算方法[J].计算机学报，2003；26(5)：611~615

6.王珏，王任等.基于 rough set 的“数据浓缩”[J].计算机学报，1998；21(5)：393~400

7.王国胤.Rough 集理论代数与信息论观点的关系研究[J].世界科技研究与发展，2002；24(5)：20~26

8.王国胤，于洪，杨大春.基于条件信息熵的决策表约简[J].计算机学报，2002；25(7)：759~766

高效的原根生成算法

作者： 夏静波， 张四兰， 陈建华， Xia Jingbo， Zhang Silan， Chen Jianhua
作者单位： 武汉大学数学与统计学院,武汉,430072
刊名： 计算机工程与应用 ISTIC PKU
英文刊名： COMPUTER ENGINEERING AND APPLICATIONS
年，卷(期)： 2006，42(11)
被引用次数： 0次

参考文献(8条)

1. 张禾瑞 近世代数 1978

2. 华罗庚 数论导引 1957

3. Eric Bach Comments on search procedures for primitive roots 1997

4. Johannes Buchmann;Victor Shoup Constructing nonresidues in finite fields and the extended Riemann hypothesis 1996(215)

5. Victor Shoup Searching for primitive roots in finite fields 1992

6. 王元 论素数的最小正原根 1959(09)

7. Guy Robin Estimation de la fonction de tchebycheff θ sur le k-ieme nombre premier et grandes valeurs de la fonction ω(n) nombre de diviseurs premiers de n 2003

8. 冯克勤 代数数论 2001

相似文献(6条)

1. 学位论文 龚克 关于最小原根的两个结果 2005

本文将利用Iwaniec筛法在代数数域和函数域两种情况下考虑最小原根的估计，介绍原根的定义及最小正原根估计方面的已有结果，并简述本文所使用的方法：引入Grossen-特征及Heckezeta函数，证明任意代数数域上的一个Perron公式，并利用Heckezeta函数的若干估计给出代数数域上的特征和估计，最后应用Iwaniec筛法改进目前最小正原根阶的估计方面的已有结果；再次利用Iwaniec筛法改进许志农在函数域上最小原根的结果，我们证明了：设P是一个系数在q元有限域F口上的一元首一不可约多项式，则模P的最小原根的次数≤6logq(degP+1)+c，其中c是任一正数.

2. 学位论文 张伟 关于十进制循环小数的一个注记 2009

设素数p≠2，5，且p以10为原根，研究1/p的十进制小数表示中的数码的规律是一个非常有趣的问题.本文的主要结果如下：

(1)设素数p≠2，5，且p以10为原根.则在1/p的十进制小数表示中的同一个循环节里，数码1，2，4，5，7，8出现的次数相同，数码0与9出现的次数相同，数码3与6出现的次数相同。

(2)设素数p≠2，5，且p以10为原根，则在q/p的十进制小数表示中的同一个循环节里，数码1，2，4，5，7，8出现的次数相同，数码0与9出现的次数相同，数码3与6出现的次数相同，其中q=1，2，3，…p-1。

3. 学位论文 卢青林 某些组合序列的同余、计数及其应用 2004

本文包括四章和一个序言，主要研究一些组合序列的同余、计数及其应用。

在第一章中我们讨论了限制性m元分拆函数b<’（s，a）>,m，j>（n）和超m元分拆函数h<,m>（n）的同余性质，其中b<’（s，a）>,m，j>（n）为将扎表示成m的幂次和的方法数，其中分拆项m<’i>允许出现的次数为a，a+s，a+2s，…，a+（i+j）s，h<,m>（n）是将n表成m的幂次和，且每个分拆项m<’i>至多重复m次的方法数。

在第二章中我们讨论了带可加性参数的广义Dyck路径（GDP）的计数问题. 我们得到了结果，这些结果推广、统一了文献中相应的结果.

在这一章的第二节中我们还指出了文献[2.8]中汁数公式的错误之处，并且给出了正确的计数公式。

在第三章里，我们讨论了与catala以数、Lucas数有关的电路问题，并且解决了Shapiro提出的一个公开问题. 我们根据电路的特性给出了“简单”函数和“线性”函数的定义，并得到如下结论，其中第一个结论回答了Shapiro的问题.

在第四章中，我们定义并研究了一般Lucas原根，它是Fibonacci原根和Lucas原根的推广. 在本章中我们给出了一般Lucas原根GLPR（m；A，B）存在的判定。

4. 学位论文 杨福祥 有限域上本原多项式的研究 2009

本原多项式的分布问题是计算数论中的一个基本问题，在密码学，编码理论，数字水印等诸多领域都有重要应用。1992年，Tom Hansen与Gary L. Mullen提出了关于Ifq上指定任意单系数的本原多项式存在性的猜想，即著名的Hansen-Mullen猜想。由于直接计算多项式系数十分困难，可以通过p-adic分析，指数和，筛不等式等工具，将其分解为一系列简单的充分条件。本文根据s. D. Cohen的工作，对指定单系数的次数高于9次本原多项式的存在性进行了研究。

本文另外对有限域上的多项式算法进行了研究，包括基本算法，不可约多项式搜索算法，多项式分解以及本原多项式搜索算法。了解本原多项式的分布情况，可以对搜索特殊性质的本原多项式起到指导作用。根据本原多项式的定义搜索本原多项式，涉及有限域上的本原根以及极小多项式的计算，时间空间复杂度很大，并且不能先验指定特定项的系数，不能作为有效的搜索算法。本文利用本原多项式的性质设计筛式算法，对候选多项式进行判定，极大减小了运算规模。这是本论文的创新点。

5. 期刊论文 郭玉秀.方贤进.韩猛.李涛 基于快速傅立叶变换的大整数乘法研究 -黑龙江科技信息2008(19)

快速傅里叶变换(FFT)是在复数域内利用单位元的n次根特性来减少运算次数,其普遍应用到高速数字信号处理.为了实现基于FFT的时间复杂度为O(nlogn)的大整数乘法运算,阐述了在p为素数或合数时;在模P运算下,如何选取适应于快速傅里叶变换的单位元的n次原根,并且给出了单位元的n次原根满足进行DFT和逆DFT运算的一些相关证明.

6.学位论文 陈华 盲签名理论研究与设计 2007

随着计算机网络及通信技术的迅猛发展，信息安全问题日益突出，其核心技术基础之一的盲签名技术，被广泛应用于电子投票、电子现金等领域，由于它具有盲性和不可链接性的特性，所以在需要实现某些参加者的匿名性的密码协议中具有其它技术无法替代的作用。

本文系统地对盲签名理论、方法和应用进行了研究，重点研究了盲签名中的若干关键技术问题，主要研究成果如下：

1. 用CAP软件实现了在盲签名中经常使用到的一些基础算法，如素性检测、原根的生成算法、大数的模幂运算、大数的模逆运算等，并研究了如何利用CAP软件对一段消息进行RSA盲签名。

2. 现有的schnorr盲化方案都是孤立提出的，缺少统一有效的盲化方法，不知道所给出的盲化方案是否是最优的。鉴于此，本文从盲化函数的代数形式入手，结合签名方程的构造特点来研究Schnorr型数字签名的一般盲化问题，提出了Sehnorr盲签名方案的一般构造方法、参数选取所应满足的条件及其导出方案，并对其安全性作了进一步的理论分析和证明，在此理论基础上，从计算时间复杂性的角度对这些方案的性能进行分析比较，从而得到该类方案中的最优方案，利用密码分析软件CAP进行简单实验，进一步说明所提方案的正确性和实际可操作性。

3. 对一个基于身份的代理盲签名方案及其安全性进行分析，证明该方案存在两个安全性缺陷，并对该方案加以改进，利用双线性映射理论，结合代理签名和盲签名的优点，将代理签名技术融入到盲签名中，提出了新型的基于身份和双线性对的代理盲签名方案；方案以身份为基础的公钥取代了以数字证书为基础的公钥，省略了验证签名时从系统中获取公钥的步骤，减少了交互的次数，节省了存储空间，并有效防止了原始签名人冒充代理签名人对消息进行签名，且限制了代理签名人的代理签名权。

4. 针对盲签名的应用，首先介绍了电子投票的一些初步知识，然后基于电子投票系统应当满足的性质，结合实际需要，设计了一种较为实用的电子投票协议。并对电子投票系统进行了系统设计，对各功能模块进行了详细设计。