文章编号:1001 - 9081(2008)05 - 1156 - 02

基于四元整数的 ElGamal 公钥密码体制

汪 丽[1],邢 伟[1],徐光忠[2]
(1. 东北大学 理学院,沈阳 110004; 2. 东软集团有限公司 商用业务部,沈阳 110179)
(wangli502521@163.com)

摘 要:介绍了既约剩余类的概念以及四元整数的一些基本性质,提出了基于四元整数群的 ElGamal 公钥密码体制(PKC),其安全性基于大整数分解和离散对数问题的困难性,并在计算机上进行模拟实现,分析了其安全性。

关键词:ElGamal 公钥密码;剩余类;四元整数; 模 n 既约四元整数同余类群
中图分类号: TP309.7 **文献标志码**:A

ElGamal public-key cryptosystem based on integral quaternions

WANG Li[1], XING Wei[1], XU Guang-zhong[2]
(1. *College of Science, Northeastern University, Shenyang Liaoning* 110004, *China*;
2. *Commercial Department, Neusoft Group Ltd., Shenyang Liaoning* 110179, *China*)

Abstract: This paper introduced the definition of congruence class and some basic property of integral quaternions, and proposed ElGamal Public-Key Cryptosystem (PKC) based on integral quaternions. Its security was based on the difficulty of large integer factorization and discrete logarithms problem. Simulation and realization were carried out in computer, furthermore the security of it was discussed and analysed.

Key words: ElGamal Public-Key Cryptosystem (PKC); residue class; integral quaternions; congrauences class group of integral quaternions mod n

比较著名的公钥密码体制主要基于两种困难问题:一是基于大整数分解问题,二是基于离散对数问题。其中比较著名的是 RSA 公钥密码体制和 ElGamal 公钥密码体制[1]。ElGamal 公钥密码体制是密码学家 ElGamal 于 1985 年提出的,由于成功应用了 Diffie-Hellman 陷门函数,一经提出便得到了广泛的应用,它主要基于有限域上离散对数的困难性。最初这个有限域是基于模 n 整数剩余类,随后文献[2]提出有限域上多项式形式的 ElGamal 体制。文献[3,4]介绍了四元整数的一些性质,提出了基于四元整数环的 RSA 公钥密码体制。受到这些启发,本文提出了基于四元整数的 ElGamal 公钥密码体制,其安全性基于大整数分解和离散对数问题的困难性,并利用 C 语言在计算机上进行了模拟实现。

1 准备知识

1.1 四元整数的一些性质

1)四元整数环

爱尔兰数学家 Hamilton 提出了四元数体,四元数体 $H \triangleq \{\alpha = a + bi + cj + dk \mid a,b,c,d \in R\}$。其中,3 个基底 i,j,k 满足:$i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$。

根据以上结论,很明显四元数满足加法和乘法的封闭性和结合律,对加法满足交换律。我们取 $h = (1 - i - j - k)/2$,如果四元数 $p = ah + bi + cj + dk$,满足条件 $a,b,c,d \in Z$(Z 为所有有理整数的集合),那么称该四元数为四元整数。

所有的四元整数组成一个环,称为四元整数环,记为 w。其中,$N(p) = a^2 + b^2 + c^2 + d^2 - a(b + c + d)$ 称为 p 的距,$N(p)$ 为整数。

2)模 n 既约四元整数同余类群

我们规定 $\alpha = ah + bi + cj + dk, a,b,c,d \in Z$ 与一个正整数 n 互素,当且仅当 α 的距 $N(\alpha)$ 与它互素,即 $(N(\alpha),n) = 1, N(\alpha) = a^2 + b^2 + c^2 + d^2 - a(b + c + d)$。

应用四元数的运算规则[3],简单地说,对于任意的四元整数 $\alpha = ah + bi + cj + dk$ 模 n,相当于 a,b,c,d 分别模 n,并且 $(\alpha \cdot \beta) \pmod n = (\alpha \bmod n) \cdot (\beta \bmod n)$ (*)。

当 $(\alpha - \beta) \equiv 0 \pmod n$ 时,称 α,β 同模。

当 n 确定时,四元整数模 n 将会组成同余类,那么每个与 n 互素的四元整数组成的同余类称为模 n 既约整数同余类,我们称所有这些四元整数同余类的全体组成的群为模 n 既约四元整数同余类群,记 $(w/n)^*$。

需要特别指出,在这个群的单位元为 $e = 2h + i + j + k$,对于任意一个 $\alpha \in (w/n)^*$, $\alpha e = e\alpha = \alpha$。

根据文献[3]我们知道,这个群为有限群,设 $\varphi(n)$ 为模 n 既约四元整数同余类群 $(w/n)^*$ 的阶,则:

$$\varphi(n) = \#((w/n)^*) = n^4 \prod_{p \mid n} (1 - 1/p)(1 - 1/p^2) \quad (1)$$

这里 p 跑遍 n 的所有有理素因子,这样 $(w/n)^*$ 就符合本文所要求的公钥密码群的条件。

2 关于四元整数环中元素乘方的计算

假设 $\alpha = a_1h + b_1i + c_1j + d_1k, \beta = a_2h + b_2i + c_2j + d_2k$,根据四元数的计算规则有:

$$\begin{aligned} h^2 &= \frac{1}{2}(-1 - i - j - k) \\ hi &= kh = h + i + k \\ hj &= ih = h + j + i \\ hk &= jk = h + k + j \end{aligned} \quad (2)$$

收稿日期:2007 - 11 - 12;**修回日期**:2008 - 01 - 02。 **基金项目**:辽宁省普通高校优秀青年骨干教师基金项目(辽宁省教育厅)。

作者简介:汪丽(1981 -),女,辽宁铁岭人,硕士研究生,主要研究方向:密码学与信息安全; 邢伟(1961 -),男,辽宁沈阳人,教授,主要研究方向:系统稳定、鲁棒控制; 徐光忠(1982 -),男,辽宁营口人,软件工程师,主要研究方向:软件开发。

通过计算,得到:$\alpha\cdot\beta=(-a_1a_2+a_1b_2+a_1c_2+a_1d_2+b_1a_2-2b_1b_2+c_1a_2-2c_1c_2+d_1a_2-2d_1d_2)h+(-a_1a_2+a_1b_2+a_1c_2+b_1a_2-b_1b_2-c_1c_2+c_1d_2+d_1a_2-d_1c_2-d_1d_2)i+(-a_1a_2+a_1c_2+a_1d_2+b_1a_2-b_1b_2-b_1d_2+c_1a_2-c_1c_2+d_1b_2-d_1d_2)j+(-a_1a_2+a_1b_2+a_1d_2-b_1b_2+b_1c_2+c_1a_2-c_1b_2-c_1c_2+d_1a_2-d_1d_2)k$。

在计算的过程中,由于四元整数乘法的计算比较繁琐,数字增长的速度比较快,根据四元整数模的计算规则(*),可以得到式(3):

$$\alpha^n(\bmod n)=\alpha^{n-1}(\bmod n)\cdot\alpha(\bmod n)\tag{3}$$

利用式(3)来计算,相对来说比较简单。

3　基本原理

3.1　密钥生成的过程

对于 n 的选择有很多,可以任意选择一个大的整数,也可以取 n 为两个素数 p 和 q 的积,或取几个素数的积,当然 n 也可以取为一个大的素数,这样计算 $\varphi(n)$ 更简单,但为了增强安全性,一般不这样取。这里为了计算 $\varphi(n)$ 方便,取 $n=pq$,当 n 很大时,分解 n 是很困难的,任意取两个大的整数 e 和 h,取 $\beta\in(w/n)^*$,计算 $y=\beta^e(\bmod n)$,$y_1=y^h(\bmod n)$,将 β,e,h,p,q 保密起来,得到公钥为 (y,y_1),解密密钥为 $\varphi(n)-h$。

3.2　加密过程

假设 A 发送消息给 B,A 获取 B 的公钥 (y,y_1),将明文消息 m 写成模 n 既约四元整数同余类 $(w/n)^*$ 中的元,即用 α 来表示。

A 随机地选取 k,计算:

$$c_1=y^k(\bmod n)\tag{4}$$

$$c_2=y_1^{\,k}\cdot\alpha(\bmod n)\tag{5}$$

于是得到密文 (c_1,c_2),将其发送给 B。

3.3　解密过程

B 收到密文后,用自己的解密密钥 $\varphi(n)-h$ 通过计算 $m=c_1^{\varphi(N)-h}\cdot c_2(\bmod n)$,得到明文 m。

3.4　基本原理

计算 m,如式(6):

$$m=c_1^{\varphi(n)-h}\cdot c_2(\bmod n)=y^{k(\varphi(n)-h)}\cdot y_1^k\cdot\alpha(\bmod n)=y^{k\varphi(n)-kh}\cdot y^{kh}\cdot\alpha(\bmod n)=y^{k\varphi(n)}\cdot\alpha(\bmod n)=\beta^{ek\varphi(n)}\cdot\alpha(\bmod n)=(\beta^{\varphi(n)})^{ek}\cdot\alpha(\bmod n)=\alpha(\bmod n)=\alpha\tag{6}$$

这里根据元素的阶的定义,$\beta^{\varphi(n)}=e$。

由于四元整数的计算比较繁琐,很难用笔算将其实现,MatLab 虽然在编写程序时代码比较少,但在实现过程中比较慢,所以本文选用 C 语言将其模拟实现。例子如下:

在 $(w/55)^*$ 群中,取 $\beta=1h+2i+3j+4k$,任意输入 E,h 的值为 17,19,选定 p,q 的值为 5 和 11,那么 β 与 55 一定互素。

那么产生的公钥为 $y=51h+34i+3j+27k$ 和 $y_1=26h+49i+18j+42k$,私钥为 6335981。

取任意的 $\alpha=4h+5i+6j+7k$ 为明文,这样通过上面得到的公钥 (y,y_1),任意的选取 $k=35$,于是得到密文 $c_1=11h+2i+18j+34k$ 和 $c_2=4h+5i+6j+7k$。

由密钥 6335981,通过计算得到明文为 $m=4h+5i+6j+7k$。具体的程序实现过程如图 1 所示。

4　安全性分析

首先,本文基于四元整数的 ElGamal 公钥密码体制。算法中公钥的计算公式为 $y=\beta^e(\bmod n)$,这里将 β 隐藏,从而破解将无法从 β 下手。另外,在已知 n 的情况下,要想破译此密码,必须得知道 h 和 $\varphi(n)$ 的值,然而这两个的计算是基于两大数学难题,计算 h 基于离散对数问题,计算 $\varphi(n)$ 基于大整数分解问题。使得攻击者很难计算出私钥,具有私钥空间的不可猜测性。

其次,如果四元整数 $\alpha=ah+bi+cj+dk$ 满足关系:

$$b=c=d=a/2\tag{7}$$

那么 $\alpha=a$,本文提出的公钥密码体制将变成原始 ElGamal 公钥密码体制,如果本文提出的密码体制被破解,那么原始的公钥密码就会被破解,又由于四元整数的乘法的计算比整数乘法繁琐,因此本文提出的算法的安全性不亚于原始的公钥密码体制的安全性。

最后,在密钥生成中,我们将不必须选取 β 为该群的生成元,若 β 不为生成元,它的阶将会小于 $\varphi(n)$,由于四元整数计算繁琐,不会为结果带来太大影响,但尽量使 β 的阶大些,p、q 应该为两个大的素数,这样分解 n 很困难;同时 ElGamal 公钥密码体制的加密算法是概率算法,它的加密实现了把明文消息均匀地分布到整个消息中,选取大的整数 n,那么 $\varphi(n)$ 将会远远大于 n,这样扩大了明文的空间,同时 e,h 的选取很自由,h 的值可以大于 n,密钥生成的任意性和加密的随机性都给攻击带来了困难性,不易泄漏消息。

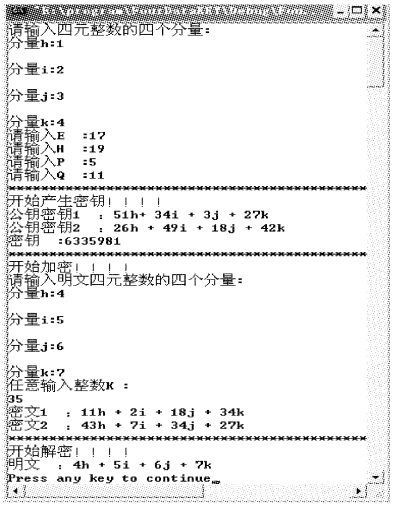

图 1　程序实现过程

5　结语

本文提出的基于四元整数的 ElGamal 公钥密码体制,加密、解密的计算过程中相对简单,具有更高的安全性,同时改进后也可用于数字签名,其理论正在研究过程中。

参考文献:

[1] MAO WEN-BO. 现代密码学理论与实践[M]. 王继林,伍前红,等译. 北京: 电子工业出版社, 2004.

[2] 张青坡, 陈彩云, 陈鲁生, 等. 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.

[3] 陆洪文. HAMILTIAN 型的解析理论: 四元数算术[J]. 中国科技大学学报,1979,9(1): 66 - 77.

[4] 陆洪文, 孙玉花. 一种四元整数公钥密码体制[J]. 同济大学学报, 2003,31(12):1463 - 1466.

[5] 潘承洞,潘承彪. 代数数论[M]. 济南: 山东大学出版社,2003.

[6] 崔苗, 姚震. 基于 ELGamal 公钥密码的算法分析与实现[J]. 福建电脑,2006(4):120 - 121.

[7] DIFFIE W, HELLMAN M E. New directions in cryptography [J]. IEEE Transation on Information Theory,1976,22(6):644 - 654.