背包公钥密码体制的数学理论研究

李步军[1]，王继顺[2]

（1.淮海工学院 理学院，江苏 连云港 222005；2.连云港高等师范专科学校 数学系，江苏 连云港 222006）

摘 要：对背包公钥密码体制的数学理论进行了研究，给出了背包单射加密函数的一个充分必要条件，以及获得单射加密函数的方法，并给出了背包公钥密码体制中的3个数学结论。

关键词：背包问题；背包公钥密码体制；单射加密函数

中图分类号：TN918.1 **文献标志码**：A **文章编号**：1673-9833(2011)05-0026-03

Mathematical Study on the Knapsack-Type Public Key Cryptosystem

Li Bujun[1]，Wang Jishun[2]

（1. School of Science，Huaihai Institute of Technology，Lianyungang Jiangsu 222005，China；
2. Department of Mathematics，Lianyungang Normal College，Lianyungang Jiangsu 222006 , China）

Abstract：The mathematical theory of public key cryptosystem is studied. The necessary and sufficient conditions for Knapsack injective and cryptographic function and the function acquiring method are presented. As a result, three mathematical conclusions in knapsack-type public key cryptosystem are obtained.

Keywords：knapsack problem；knapsack-type public key cryptosystem；injective and cryptographic function

1 研究背景

1949年，C. E. Shannon发表了《保密系统的通信理论》一文，使密码学成为一门真正的科学。作为一门应用性较强的学科，密码学有坚实的数学理论基础，在代数学、数论等知识的基础上，出现了基于多项式理论的序列密码，基于数论知识的RSA[1]和EIGamal等公钥密码。

背包密码[2]是一种基于背包问题的公钥密码，该问题就是从背包向量$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$（$a_i \in \mathbf{Z}^+$）中求出所有的$a_i$，使其和等于给定的正整数$b$。背包问题是一个NP完全问题[3]，背包公钥密码体制的安全性就是基于该问题的难解性。然而对于超递增的背包向量[4]，却存在解决问题的简单方法。

在实际应用中，加密者首先使用公钥$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$，通过计算$b=f_a(x)=x_1a_1+x_2a_2+\cdots+x_na_n$，对明文$x=x_1,x_2,\cdots,x_n$，$x_i \in \{0,1\}$进行加密，然后将密文$b$发送给信息接收者，接收者利用其私钥可将密文恢复为明文。而对密码系统的攻击相当于解决一个背包问题。本文对背包公钥密码体制问题从数学理论方面作些探讨。

2 主要结论

如果背包问题存在多个解，这时密文b就对应多个明文，解密后信息接收者会得到不确定的明文，因此要求加密函数$f_a(x)=x_1a_1+x_2a_2+\cdots+x_na_n$是单射，定理1将给出背包单射加密函数的一个充分必要条件。

收稿日期：2011-05-26
基金项目：淮海工学院特色专业建设基金资助项目（5509007）
作者简介：李步军（1971-），男，山东临沂人，淮海工学院讲师，硕士，主要研究方向为信息安全及系统分析，
E-mail：lbjbjls@yahoo.com.cn

定理 1　函数$f_a(x)=x_1a_1+x_2a_2+\cdots+x_na_n$（$a_i\in\mathbf{Z}^+$）是单射（$\boldsymbol{A}$为单射背包向量）的充分必要条件为：背包向量$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$的每 2 个分量 a_i,a_j 都不相等，且每个分量都不能表示成其它若干分量的和或差。

证明　用反证法

1）必要性

若背包向量$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$有两个分量$a_i,a_j$相等，设它们对应的系数$x_i$, x_j不相等，则

$$f_a(x_1x_2\cdots x_i\cdots x_j\cdots x_n)=f_a(x_1x_2\cdots x_j\cdots x_i\cdots x_n),$$

因此函数$f_a(x)$不是单射。

若$a_i=a_j+a_p-a_q$，则存在第i,q位为 1，其余位为 0 的二进制串，以及j,p位为 1，其余位为 0 的二进制串，这 2 个二进制串的函数值相等，因此函数$f_a(x)$不是单射。

必要性得证。

2）充分性

假设函数$f_a(x)=x_1a_1+x_2a_2+\cdots+x_na_n$不是单射，则存在 2 个不同的二进制串$x=x_1x_2\cdots x_n$和$x'=x_1'x_2'\cdots x_n'$满足$f_a(x)=f_a(x')$，即

$$x_1a_1+x_2a_2+\cdots+x_na_n=x_1'a_1+x_2'a_2+\cdots+x_n'a_n。\qquad(1)$$

假设方程（1）两边背包向量$\boldsymbol{A}$的分量a_i系数相同的项的个数有且只有p个（$p<n$，$p\in\mathbf{Z}^+$），不妨设是前p个，即$x_1=x_1'$，$x_2=x_1'$，…，$x_p=x_p'$，则方程（1）可以化为

$$x_{p+1}a_{p+1}+x_{p+2}a_{p+2}+\cdots+x_na_n=x'_{p+1}a_{p+1}+x'_{p+2}a_{p+2}+\cdots x'_na_n,\qquad(2)$$

方程（2）两边对应a_i（$i=p+1,p+2,\cdots,n$）的系数不相同，即$x_{p+1}\neq x'_{p+1}$，$x_{p+2}\neq x'_{p+2}$，…，$x_n\neq x'_n$。

不妨设$x_{p+1}x_{p+2}\cdots x_{p+r}x_{p+r+1}\cdots x_{n-1}x_n=00\cdots01\cdots11$，则$x'_{p+1}x'_{p+2}\cdots x'_{p+r}x'_{p+r+1}\cdots x'_{n-1}x'_n=11\cdots10\cdots00$。

此时方程（2）化为

$$a_{p+r+1}+a_{p+r+2}+\cdots+a_n=a_{p+1}+a_{p+2}+\cdots+a_{p+r},$$

因此

$$a_{p+r+1}=a_{p+1}+a_{p+2}+\cdots+a_{p+r}-a_{p+r+2}-\cdots-a_n,$$

即a_{p+r+1}可以表示成$a_{p+1},a_{p+2},\cdots,a_{p+r},a_{p+r+2},\cdots,a_n$的和或差，这与已知条件矛盾。

充分性得证。

只要密码体制使用者选择单射背包向量$\boldsymbol{A}$作为其公钥，就可以保证至多存在一个背包问题的解决方案。

推论 1　超递增向量$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$（$a_i\in\mathbf{Z}^+$，$a_i>a_1+a_2+\cdots+a_{i-1}$，$i\geqslant 2$），是单射背包向量。

证明　1）显然超递增向量中的每 2 个元素都不相等。

2）再证$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$中的每一个元素都不能表示成其它若干个元素的和或差。

假设$a_i=a_j+a_p-a_q$，则$a_i+a_q=a_j+a_p$。由于a_i,a_j,a_p,a_q中一定有一个最大者，不妨设a_j最大，从而a_i,a_p,a_q必在a_j前面。由于a_j比它前面所有项的和还大，所以$a_j>a_i+a_p+a_q$，这与$a_i+a_q=a_j+a_p$矛盾。

根据 1），2）和定理 1，推论 1 得证。

定理 2　设$\boldsymbol{C}=(c_1,c_2,\cdots,c_n)$（$c_i\in\mathbf{Z}^+$），为$n$维超递增的背包向量，正整数$m,t$互素且$m>c_1+c_2+\cdots+c_n$，则由模乘运算$a_i=tc_i\%m$对$\boldsymbol{C}=(c_1,c_2,\cdots,c_n)$伪装后所得向量$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$为单射背包向量。其中$tc_i\%m$表示$tc_i$除以$m$后所得的余数。

证明　1）先证背包向量$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$中任意 2 个分量都不相等。

假设背包向量$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$中有 2 个分量$a_i=a_j$，即$tc_i\%m=tc_j\%m$。

不妨设$c_j>c_i$，则$tc_j-tc_i=km$, $k\in\mathbf{Z}^+$，因此$c_j-c_i=km/t$。因为m,t互素，所以有t整除k，令$k/t=n$，则$c_j-c_i=mn$，$n\in\mathbf{Z}^+$。

所以$c_j-c_i=mn\geqslant m>c_1+c_2+\cdots+c_n>c_j$，即$c_j>c_j+c_i$，自相矛盾。

因此，假设不成立，1）证毕。

2）再证背包向量$\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$中的每个分量都不能表示成其它若干分量的和或差。

假设$a_i=a_j+a_p-a_q$，即

$$tc_i\%m=tc_j\%m+tc_p\%m-tc_q\%m,$$

则有$tc_i\%m+tc_q\%m=tc_j\%m+tc_p\%m$，

因此tc_i+tc_q和tc_j+tc_p必相差m的整数倍。

不妨设$tc_i+tc_q\geqslant tc_j+tc_p$，令

$tc_i+tc_q-tc_j-tc_p=km$，$k\geqslant 0$，$k\in\mathbf{Z}$，即

$c_i+c_q-c_j-c_p=km/t$。

因为m,t互素，所以t整除k，令$k/t=n$，则

$c_i+c_q-c_j-c_p=mn$，$n\geqslant 0$，$n\in\mathbf{Z}$。

当$n>0$时，

$c_i+c_q-c_j-c_p=mn\geqslant m>c_1+c_2+\cdots+c_n>c_i+c_q$，即

$c_i+c_q>c_i+c_q+c_j+c_p$，矛盾。

当$n=0$时，$c_i+c_q-c_j-c_p=0$，即$c_i=c_j+c_p-c_q$。

由定理 1 知$\boldsymbol{C}$不是单射背包向量，这与已知条件和推论 1 矛盾。

根据 1），2）和定理 1，定理 2 得证。

由一元单射函数和背包线性加密函数的特点可得定理 3。

定理 3[5-6]　设$y=h(u)$为一元单射函数，其定义域为D_h，$u=f_a(x)=x_1a_1+x_2a_2+\cdots+x_na_n$为$n$元背包单射加密函数，其值域为$R_f$，且$R_f\subseteq D_h$，则复合函数$y=h[f_a(x)]$为单射加密函数。

由定理3可知，由多元单射线性加密函数和一元非线性单射函数复合后，可得多元非线性单射加密函数。

3 结语

本文对背包公钥密码体制问题给出了3个定理，其中定理1给出了背包单射加密函数的一个充要条件，定理2是设定私钥和公钥的理论依据，定理3为探索组合型加密方法提供了一种思路。定理3中，如果$y=h(u)$选取适当（即函数不易求逆），利用$y=h[f_a(x)]$加密时，背包公钥密码体制的安全性会提高，这值得学者们进一步研究和探索。

参考文献：

[1] 陈鲁生，沈世镒. 现代密码学[M]. 北京：科学出版社，2002：73-75，86-88.
Chen Lusheng，Shen Shiyi. Modern Cryptography[M]. Beijing：Science Press，2002：73-75，86-88.

[2] 王宝仓，韦永壮，胡予濮. 基于随机背包的公钥密码[J]. 电子与信息学报，2010，32(7)：1580-1584.
Wang Baocang，Wei Yongzhuang，Hu Yupu. Public Key Cryptosystem Using Random Knapsacks[J]. Journal of Electronics & Information Technology，2010，32(7)：1580-1584.

[3] 吕国英. 算法设计与分析[M]. 北京：清华大学出版社，2006：39-40.
L ü Guoying. Algorithm Design and Analysis[M]. Beijing：Tsinghua University Press，2006：39-40.

[4] Paul Garrett. 密码学导引[M]. 吴世忠，宋晓龙，译. 北京：机械工业出版社，2003：141-143.
Paul Garrett. Making, Breaking Codes: An Induction to Cryptography[M]. Wu Shizhong，Song Xiaolong，Translator. Beijing：Machinery Industry Press，2003：141-143.

[5] 孟广武，张晓岚. 高等数学[M]. 上海：同济大学出版社，2006：7-9.
Meng Guangwu，Zhang Xiaolan. Higher Mathematics[M]. Shanghai：Tongji University Press，2006：7-9.

[6] 邓胜兰. 抽象代数基础[M]. 北京：机械工业出版社，2011：11-13.
Deng Shenglan. The Basis of Abstract Algebra[M]. Beijing：Machinery Industry Press，2011：11-13.

（责任编辑：邓光辉）

（上接第25页）

[10] 吴 彬，王万录，廖克俊，等. 退火处理对透明导电$CdIn_2O_4$薄膜光学、电学性质及其能带结构的影响[J]. 半导体学报，1997，18(2)：151-155.
Wu Bin, Wang Wanlu, Liao Kejun, et al. Effect of Annealing Treatment on Optical, Electrical Properties and Energy Structure of Transparent Conductive $CdIn_2O_4$ Thin Films [J]. Chinese Journal of Semiconductors，1997，18(2)：151-155.

[11] 陈 猛，白雪冬，黄荣芳，等. In_2O_3：Sn和ZnO：Al透明导电薄膜的结构及其导电机制[J]. 半导体学报，2000，21(4)：394-399.
Chen Meng, Bai Xuedong, Huang Rongfang, et al. Structure and Conductive Mechanism of ITO and ZAO Films[J]. Chinese Journal of Semiconductors，2000，21(4)：394-399.

[12] 陈艳伟，于文华，刘益春. 热处理对ZnO：Al薄膜的结构、光学和电学性质的影响[J]. 中国科学：G辑，2004，34(3)：345-353.
Chen Yanwei, Yu Wenhua, Liu Yichun. Effect of Annealing on Structural, Optical and Electrical Properties of Al-Doped ZnO Thin Films[J]. Science in China：Series G, 2004, 34 (3)：345-353.

[13] 陈 欣，方 斌，官文杰，等. 沉积温度和退火处理对脉冲激光沉积的ZnO：Al膜性能的影响[J]. 功能材料，2005，36(10)：1511-1513.
Chen Xin，Fang Bin，Guan Wenjie, et al. Influence of Substrate Temperature and Post-Treatment on the Properties of ZnO:Al Thin Films Prepared by Pulsed Laser Deposited [J]. Journal of Functional Materials，2005，36(10)：1511-1513.

[14] J Fang Guojia, Li Dejie, Yao Baolun. Influence of Post-Deposition Annealing on the Properties of Transparent Conductive Nanocrystalline ZAO Thin Films Prepared by RF Magnetron Sputtering with Highly Conductive Ceramic Target[J]. Thin Solid Films，2002, 418(2)：156-162.

（责任编辑：李玉珍）