毕业论文中期检查报告

论文题目：格算法在背包公钥密码体制分析中的应用

指导教师：陆正福（教授） 报告人：白文寿

1. 背包问题：指给定一个正整数的集合{b1,b2,···,}和一个整数S，找一个0,1向量{x1,x2,···,},使得.背包问题可能有多解、没有解或者唯一解的情况，所以它是个NP问题。

2、超递增序列：如果一个正整数序列满足条件，称为超递增序列。

3、基本Merkel-Hellman体制

(1)选取一个超递增背包和模使；

(2)取使，并求满足的；

(3)构造背包向量且；

(4)公钥:，私钥：、和；

(5)加密

设明文；

密文；

(6)解密

收到密文后，计算，收方由利用

的超递增特性可求出明文；由于是保密的，非法用户不能由还原

.

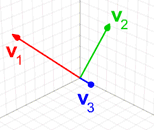
4、格基规约算法：

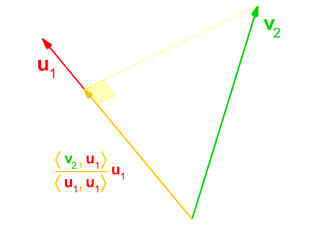
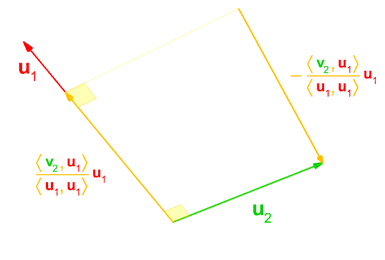
①Gram-Schmidt正交化

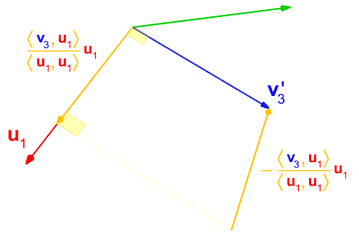
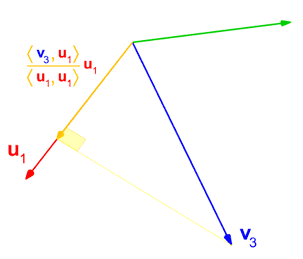
Step1：

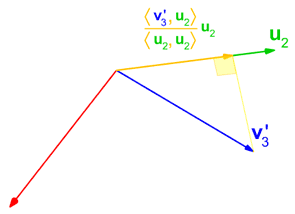
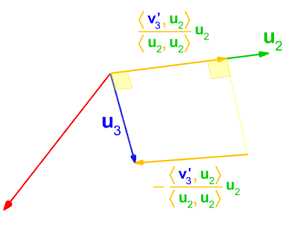
Step2：，其中

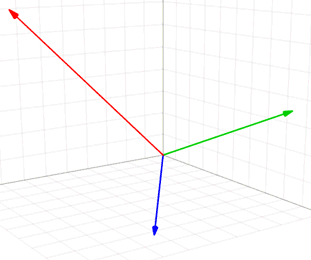
\*三维正交化图形实例：





②LLL规约算法

输入：格L的一组基和规约参数

输出：以参数规约的LLL规约基

1：k=2；

2:while(k<=n){

2.1:计算Gram-Schmidt正交化系数和 ；

2.2：for(j=1;j<k;j++){

ifthen 

else 

};

2.3:;

2.4:if(){

2.4.1:交换和；

2.4.2：；

}else ；

}；

3：输出.

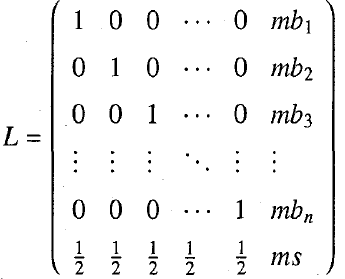
1. 用LLL算法求解子集和问题时解的确定

（1）输入：一个正整数集合和整数S

输出：，满足，假设存在

①、计算

②、下列矩阵L的行向量组成一组基，有这组基生成维格



③、利用LLL算法求解的约化基B

④、对B中的每一个向量，执行

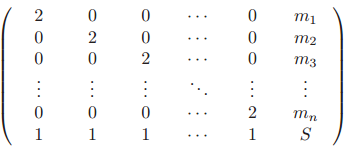
\*若对所有的，有且，执行以下操作：

对，令，如果，则返回一个解

对，令，如果，则返回一个解

（2）假设要破解为S，密文为

①构造出一个(n+1)维矩阵L



②对矩阵L进行规约得到规约矩阵

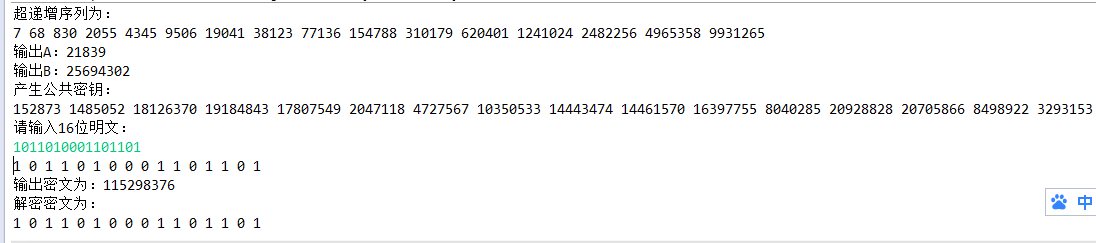
③在矩阵中选择最后一个值为0，并且其他数全为1或-1的行，

其中

④假设明文为，那么

实验截图

1、Merkel-Hellman的实现：



2、LLL算法的实现：还没调试成功

