密码学作业006 学号 20131910023 姓名 金洋

格与密码学的问题  
1. 什么是格?

答：令∈是一组线性独立的向量，则称为由产生的格；

2. 格与子空间的区别是什么?

答：定义1(子空间) 数域P上线性空间V的一个非空子集合W称为V的一个线性子空间或简称子空间，如果W对于V的两种运算加法和数乘也构成线性空间.

定义2(生成子空间) 设，则子空间 

即这组向量所有的线性组合构成的子空间,称为由生成的子空间，记作. 称为它的一组生成元.

综上可以看出，格与子空间的区别在于基的线性组合的系数所在的系数不同，格的系数必须为Z，而子空间的系数取决于定义时的数域P。

3. 欧氏空间正交化算法的输入与输出分别是什么?

答：Input：向量空间上的一组基；

Output：上的一组正交基；

4. 欧氏空间正交化算法的不变量或不变式是什么?变化的是什么？

答：不变：，两组基有相同的行列式，,基向量在正交坐标轴上的投影；

变化：原本不正交的基；

5. 分析欧氏空间正交化算法的复杂度。

答：设欧式空间是n维的，则算法复杂度为；

6. 比较格中最短向量问题与码中最小重量码字问题。

答：格中最短向量问题：在格中寻找一个非零的最短向量。

最小码重问题：在一个码字集合中,寻找一个非零码元的个数（汉明重量）最少的码字；

后者可以通过计算出每个码字的汉明重量，具有最小重量的码字记为结果。

前者的基若是充分正交，那么最短向量就一定在集合中，若基是一组坏基，且维数一大，该问题就成为NP难问题。

1. 简述Babai算法的输入、输出、设计思路。

答：Input：一组好基，

Output：在格中的最短向量；

设计思路：设，现在希望求得在格中的最短向量，

即需要取到最小值；

又由于是一组好基，，则只需令每个（上下取整），即可使得取到最小值。

8. 分析Babai算法的复杂度。

答：需要把用格上的基表示出来，运用高斯消元法——；

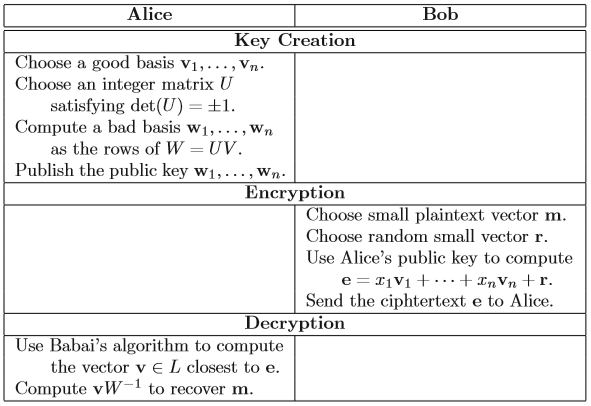
在对每个基向量的系数上下取整——；

所以算上高斯消元Babai算法的复杂度为；

若不算高斯消元，算法复杂度为；

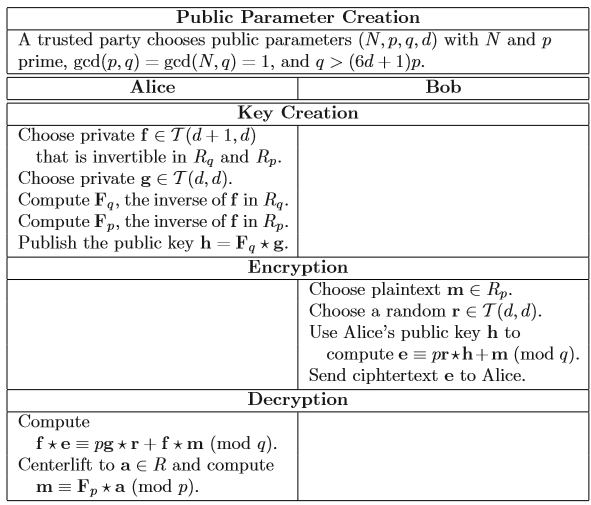
9. 简述GGH密码体制。

答：GGH是格上的公钥密码体制，它的安全性依赖于格中最近向量问题。具体实现如下：



10. 简述NTRU密码体制。

答：这是一个基于多项式环的密码体制。它的安全性依赖于格中最短向量问题（SVP）。相对于离散对数或大数分解等公开秘密体制来说，它有许多优势——与现有流行密码体制相比，满足相同安全性只需要更小位数的密钥量、对计算机计算性能要求不高、加解密速度快。在安全性方面，NTRU算法具有抵抗量子计算攻击的能力。



11. 格基归约算法的不变式是什么？变化的是什么？

答：对于高斯格规约算法——

不变：基中长度较短的那个向量，不妨设；

变化：基中较长向量若在上的投影长度超过，则做出变化。

对于3L格基规约算法——

不变：，满足Lovasz条件和size条件的基；前后两组基构成的行列式的值；

变化：不满足3L条件的基向量；