# 第七届（2022 年）全国高校密码数学挑战赛

# 赛题二

## 一、赛题名称：隐藏数问题(Hidden Number Problem)的求解

## 二、赛题描述

### 2.1 符号说明

记$\mathbb{Z}$是整数环，$q\in\mathbb{Z}$为$m$比特的正整数, 即$m=[\log_2 q]$. $\mathbb{Z}/q\mathbb{Z}$是模$q$剩余类环. 对$a,b\in\mathbb{Z}$, $a\equiv b(\bmod q)$表示$a,b$属于同一个模$q$剩余类中，即$q\mid a-b$.

### 2.2 基础知识

取定$\mathbb{Z}/q\mathbb{Z}$的一个完全剩余系$\{0,1,\cdots,q-1\}$，即把$\mathbb{Z}/q\mathbb{Z}$中剩余类的代表元取为$\{0,1,\cdots,q-1\}$中的元素.

此时, 对$b\in\{0,1,\cdots,q-1\}$，可设

$$b=\sum_{i=0}^{m-1}b_i2^i,\quad b_i\in\{0,1\}.$$

把$b$表示成$m$长的二进制比特串$(b_{m-1},b_{m-2},\cdots,b_0)$，其中左面的比特称为$b$的高比特分位，右面的比特称为$b$的低比特分位.

### 2.3 问题描述

设$x_0\in\mathbb{Z}/q\mathbb{Z}$是未知变元, 称之为**隐藏数**.

在$\mathbb{Z}/q\mathbb{Z}$中随机一致的选取$n$个元素(已知)，记为向量$\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in(\mathbb{Z}/q\mathbb{Z})^n$. 令$\beta_i\equiv\alpha_i x_0(\bmod q), 1\le i\le n$，$\beta=(\beta_1,\beta_2,\cdots,\beta_n)\in(\mathbb{Z}/q\mathbb{Z})^n$, 得到环$\mathbb{Z}/q\mathbb{Z}$上单变元线性方程组

$$\alpha x_0\equiv\beta(\bmod q),$$

其中β为方程组的常数项,并假设$\beta$的分量$\beta_i$表示为$m$长比特串时,其中只有部分固定的分位比特已知.

对上面线性方程组，在方程组系数$\alpha$已知，而常数项$\beta$的分量只有部分比特信息已知时,试求解未知的隐藏数$x_0$,就是**隐藏数问题.**

在下面的问题中，我们只考虑$q=2^m$为2的方幂和$q$为一$m$比特素数这两种情况.

当$q=2^m$时，由于$\beta_i$低比特分位只与$x_0$和$\alpha_i$的低比特分位有关，我们只考虑$\beta_i$高$s$比特分位已知的情形，此时简记为HNP-($m,s$).

而当$q$为素数时,可以考虑其它位置比特已知的情形.

## 2.4 赛题描述和成绩评判标准

本竞赛题目分为三个部分,共 200 分:

1.（20’）掌握 HNP 格求解算法的基本原理、格模型构建和算法求解能力.

在固定参数$(m,s)$下，试在理论上分析格方法求解 HNP-$(m,s)$所需的最小方程量$n$(即所需存在比特泄露的$\alpha_i$的最小个数).验证 HNP 格求解算法的实际求解能力是否与理论分析结果相符合,分析现有格算法求解 HNP 的能力极限.

2. （150’）尝试求解**附件**中给出的10个HNP，求出每个问题的隐藏数$x_0$.

十个问题中的(1)，(5)-(10)这七个问题中，模数$q=2^m$，每

个$\beta_i$的高$s$比特已知．参数$(m,s)$分别为：（1）（256, 8），（5）（256, 4），(6)（384, 6），(7)（160, 2），(8)（224, 2），(9)（384, 3），(10)（128, 1）.

问题(2)-(4)这三个问题的模数$q$是素数，其中，

问题(2)中$q$为$256$比特素数，每个$\beta_i$的最低 8 比特为已知;

问题(3)中$q$为$512$比特素数，每个$\beta_i$的最高 128 比特和最低 360 比特未知，中间 24 比特为已知;

问题(4)中$q$为$512$比特素数，每个$\beta_i$的$512$比特分为 5 段，其中最高 154 比特、最低 154 比特和中间的 154 比特未知，其余两段各 25 比特为已知.

**数据格式说明**：每题开始给出该题目的具体参数，$q$为模数，$s$为已知比特分位数，$n$:=EquaNum 为方程量，Coeff 表示$n$维系数向量$(\alpha_1,\alpha_2,\cdots,\alpha_n)$，KnownNonce 表示$n$维常数项已知比特分位的值．注意在(4)题中，KnownNonce 的每个元素的两个分量分别为已知的两段 25 比特的值，按[高 25 比特，低 25 比特]的顺序存放.

**注记**：题目中，$(\alpha_1,\alpha_2,\cdots,\alpha_n)$和对应$\beta_i$的已知$s$比特信息均用**十进制数据**表示，即每个$\alpha_i$表示成$0\sim(q-1)$之间的整数，而$\beta_i$的已知$s$比特表示为$0\sim(2^s-1)$之间的整数(比特分位左高右低).

每题分值如下：(1)5’，(2)5’，(3)10’，(4)10’，(5)15’，(6)15’，(7)15’，(8)20’，(9)25’，(10)30’.

3.（30’）对求解 HNP 在理论和方法上有创新性研究．例如构建出

求解 HNP 的新模型，效果能达到或超过现有格方法的求解能力;

对仅已知 1 比特的 HNP，设计高效求解算法等.

## 三、密码学背景及相关问题的研究进展

为了研究 Diffie-Hellman 密钥交换体制私钥的比特安全性(bit-security)，D.Boneh 和 R.Venkatesan 等人在 1996 年的美密会上最先提出了隐藏数问题(Hidden Number Problem，简记为 HNP)，并通过构建格模型给出求解 HNP 的一种确定性算法，以此证明了 DH 体制中私钥的部分比特与整体比特安全性之间存在归约关系（见参考文献[1]）.

后来，P.Q.Nguyen、I.E.Shparlinski 等人利用 HNP 格求解方法，研究了数字签名算法(Digital Signature Algorithm，简记为 DSA)在部分私钥比特已知时的体制安全性（见参考文献[2]）. DSA 是美国国家标准与技术局(NIST)推荐使用的签名算法之一，已经证明DSA的安全性等价于有限域上离散对数求解问题. 但是,如果用户私钥存在部分比特泄露，即存在 Partially Known Nonces 时，DSA 的安全性就很可能出现问题. 类似的, ECDSA、ElGamal 等密码体制的私钥如果存在比特泄露的情形，也可能使用 HNP 方法求取私钥.

在现实中,存在多种用户私钥出现部分比特泄露的可能原因,包括随机数生成算法缺陷、侧信道攻击暴露等.近年来,利用侧信道方法攻击密码安全性的实例经常出现,其中某些利用到了 HNP 的求解.

在文献[1]和[2]中，通过构建合适的格模型,可以把常数项高比特分位已知的 HNP 求解转化为格中 CVP 和 SVP 的求解. 这样,HNP 的求解

能力就取决于相应格算法的运行效率. 近期, 随着 BKZ2.0 以及格筛法等格算法研究的推进, HNP 的求解能力也有了较大的提升.

通常认为,格方法只适合于已知信息大于 1 比特的情形,而对仅已知 1 比特的 HNP,文献[3]给出了一个理论上的求解方法.

本赛题设计了 HNP 及其变形的若干情况, 希望参赛队员能在理解现有 HNP 求解算法的能力及其局限的基础上, 激发研究兴趣, 拓展 HNP 的相关研究工作.

## 四、参考文献

**[1]** Boneh, D. and Venkatesan, R., "*Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes*," in Koblitz, N. (ed.) Advances in Cryptology - CRYPTO '96. LNCS, vol.1109, pp.129-142, Springer, Heidelberg, 1996.

**[2]** Nguyen, P.Q. and Shparlinski, I.E. , "*The Insecurity of the Digital Signature Algorithm with Partially Known Nonces,*" in Journal of Cryptology, 15(3), pp.151-176, 2002.

**[3]** Akavia, A., "*Solving Hidden Number Problem with One Bit Oracle and Advice*," in Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009. LNCS, vol.5677, pp.337-354, Springer,Heidelberg，2009.