第五届（2020）全国高校密码数学挑战赛
赛题三

一、赛题名称：子集和问题

二、赛题描述

2.1 问题描述

子集和问题是指给定 n+1 个正整数 $a_0, \ldots, a_{n-1}$ 和 s，求解 n 个未知数 $x_0, \ldots, x_{n-1}$，其中，对于 i=0, …, n−1，x_i=0 或 1，使得 $a_0x_0+\ldots+a_{n-1}x_{n-1}=s$.

2.2 竞赛要求成和绩评判标准

1) 本赛题共分 9 级挑战，每级挑战 4 道题（见赛题三附件）。

2) 每道题目均给出了五个参数：子集和问题维数 n、子集和密度 d（定义见第三部分）、子集和向量 $\mathbf{a}=(a_0, \ldots, a_{n-1})$、和值 s、以及推荐的子集和问题解向量 $\mathbf{x}=(x_0, \ldots, x_{n-1})$的汉明重量 k（定义见第三部分）。待求解的子集和问题的解可能不唯一，选手若求解出的解向量 **x** 的汉明重量不为 k 同样得分。

3) 每级挑战参赛选手只需选作一道题目，多做题目按照得分最高的那道题目计分。

4) 每级挑战的基准分值见表 1。

表 1. 每级挑战分值

挑战级	1	2	3	4	5	6	7	8	9
基准分值	200	400	600	800	1000	1200	1400	1600	1800

5) 选手每级挑战的成绩计算规则如下：选手第 i 级题目的基准分

值为 J_i，选手第 i 级挑战得分记为 S_i。若选手正确求解了第 i 级挑战（即，正确求解出了子集和问题的一个解，不要求解出的解的汉明重量是 k），则得分 S_i 为对应等级挑战的基准分值 J_i。若选手未求解出某一级挑战赛的 0-1 解，该等级的分数按照选手求解出的方程 $a_0x_0+\ldots+a_{n-1}x_{n-1}=s$ 的整数解向量 $\mathbf{x}=(x_0, \ldots, x_{n-1})$的欧几里得范数$\|\mathbf{x}\|_2=\sqrt{x_0^2+\cdots}$ 的大小来计算，得分计算公式为

$$S_i=\text{基准分值 } J_i/2+k-\|\mathbf{x}\|_2^2。$$

每级挑战最低得分为 0 分。

6) 针对每级挑战，给出计算平台和计算结果，并简述求解原理、步骤和实现效率（包括计算需要的时间和空间等）；

7) 提出前人未提出过的新型求解算法的，酌情加分。

三、密码学背景及相关问题的研究进展

公钥密码的基本思想就是在数学困难问题中嵌入陷门信息，使得非授权用户不能通过求解困难问题来获取加密信息，而拥有陷门信息（私钥）的用户可以使用私钥解密密文重构明文信息。子集和问题已经被证明是 NP-完全问题，因此，1978 年，研究人员就使用该问题构造了一个公钥加密算法——Merkle-Hellman 算法（注：Merkle 和 Hellman 误用了子集和问题和背包问题的概念，在密码学中，这两个问题都是指子集和问题）。

在 P≠NP 的基本假设下，不可能找到求解子集和问题的多项式时间算法。但是，精心设计的求解算法往往能降低求解的计算复杂度。

比如说，穷举 x_i=0 或 1 的值，需要 $O(2^n)$的计算量；而使用生日攻击来求解该问题，可以把计算量进一步降低至 $O(n2^{0.5n})$；2010 年和 2011 年的欧洲密码学年会上，研究人员进一步降低了子集和求解问题的计算复杂度[1]。

受子集和公钥密码分析的驱动，研究人员也尝试使用格归约的方法求解子集和问题，比如 LLL 算法、BKZ 算法等，选手可以在如下链接中找到几类格归约算法的程序，https://www.shoup.net/ntl/。比如，Coster 等人证明了[2]，当背包密度 $d=n/\log_2\max\{a_1, \ldots, a_n\}<0.9408$ 时，子集和问题的解以极大的概率可以通过寻找某个格上的最短向量来求解；Ping 等人证明了[3]，低重量（指子集和问题的解向量$(x_0, \ldots, x_{n-1})$的汉明重量，即解向量中 1 的个数 $k=|x_0|+\ldots+|x_{n-1}|$比较小）、高密度背包密码中的子集和问题可以确定性的归约到格上的最短向量问题。

四、参考文献

[1] Becker A., Coron J., Joux A., Improved generic algorithms for hard knapsacks, in Advances in Cryptology-EUROCRYPT 2011, Tallinn, Estonia, May 15-19, 2011 (LNCS, 6632), pp. 364-385.

[2] Coster M.J., Joux A., LaMacchia B.A., et al., Improved low-density subset sum algorithms, Computational Complexity, 1992, 2, (2), pp. 111-128.

[3] Yuan Ping, Baocang Wang, Shengli Tian, Yuehua Yang, Genyuan Du, Deterministic lattice reduction on knapsacks with collision-free properties, IET Information Security, 2018, 12(4), pp. 375-380.