第二届（2017）全国高校密码数学挑战赛

赛题四

一、赛题名称：极大布尔多项式方程组可满足问题

二、赛题描述：

1.1 基本概念

二元域：GF(2)为含有两个元素0,1的有限域。元素0,1满足如下加法与乘法性质，0+0=0, 0+1=1, 1+1=0, 0*0=0, 0*1=0, 1*1=1。

布尔多项式：系数在GF(2)上的多变量多项式，若其含有n个变量$x_0, x_1, \cdots, x_{n-1}$，则该多项式的每个单项式中的$x_i$的次数小于等于1次。例如：$x_0x_1+x_1x_2+x_0x_1x_2+x_2+1$为一个含有3个变量的布尔多项式。

1.2 问题描述（Max-PoSSo问题）

给定m个含有n个变量的布尔多项式

$f_0(x_0, x_1, \cdots, x_{n-1})$, $f_1(x_0, x_1, \cdots, x_{n-1}), \cdots, f_{m-1}(x_0, x_1, \cdots, x_{n-1})$,

寻找一组$x_0, x_1, \cdots, x_{n-1}$的赋值，其中每个$x_i$的取值均在GF(2)中，使得$f_0, f_1, \cdots, f_{m-1}$在这组变量赋值下取值为0的个数最多。（注：在本次竞赛问题中，m=256, n=128, $f_0, f_1, \cdots, f_{255}$为给定的256个布尔多项式）

1.3 成绩评判

将各参赛组给出的变量赋值代入$f_0, f_1, \cdots, f_{m-1}$中，得到取值为0的多项式的个数k。该题为2016年赛题一,k值需要大于上一届比赛冠军队伍给出的值234。评判注重k值的大小或能否说明k最优、方法上是否有创新。

三、密码学背景及相关问题的研究进展

布尔多项式方程组求解是数学与计算机科学中的基本问题之一。该领域最基本的问题是一般布尔多项式方程组求解问题（PoSSo问题），即给定一组布尔多项式，寻找变量赋值使得这些多项式取值均为0。上述极大布尔多项式方程组可满足问题（Max-PoSSo问题）是一般布尔多项式方程组求解问题的扩展问题，是一类NP-hard问题。该问题在密码学的概率代数攻击与侧信道代数攻击中广泛出现。

在密码分析中的代数攻击中，攻击者首先将秘密信息（如密钥）设为变量，之后通过已知信息与秘密信息的关系建立相应的多项式方程组，最终通过求解多项式方程组来恢复秘密信息。然而，在多项式方程组的建立过程中，一些概率假设以及通过物理手段获取信息中出现的噪声，会造成需要求解的多项式方程组的某些项(一般为常数项)出现一定的错误，造成多项式组无法同时取值为0。此时，

为了恢复秘密信息，攻击者需要寻找使得方程成立个数最多的解，而该解有很大概率就是未出现错误的方程组的解。

对于极大布尔多项式方程组可满足问题，现有的求解方法不是很成熟，有很大的研究空间。现有的主要的求解思路有两类。

1) 遍历变量取值。此类方法的思想是通过遍历变量取值并结合一些减少搜索分支策略来寻找最优的变量赋值。由于在一些其他数学问题中，基于遍历搜索思想的算法开发较为成熟，因此，我们可以利用一些代数变换，将Max-PoSSo问题转化为一些有成熟求解算法的问题，例如转化为混合整数规划问题（MIP问题），之后通过相应的求解器来求解转化后的问题[1]。此时，需要研究的是如何有效将Max-PoSSo转化为其他问题，使得求解效率更高。
2) 遍历多项式取值。固定每个多项式的取值，求解对应的一般布尔多项式方程组。若能找到使得对应一般多项式方程组有解，且0的个数最多的多项式取值，则该一般多项式方程组的解是Max-PoSSo问题的解。在 [2,3]中，作者基于此思想给出一种基于回溯搜索多项式取值与递增求解代数系统思想的算法。在求解一般布尔多项式方程组方面，现有的较有效的算法有Groebner基方法[4]、SAT方法[5]、特征列方法[6]。此时，需要研究的问题是如何将代数求解算法与搜索策略有效结合，减少搜索分支并提高单分支的求解效率。

四、参考文献

[1] Albrecht, M.R. and Cid, C.: Cold Boot Key Recovery by Solving Polynomial Systems with Noise. ACNS 2011: 57-72.
[2] Huang, Z. and Lin, D.: A New Method for Solving Polynomial Systems with Noise over F2 and Its Applications in Cold Boot Key Recovery, Selected Areas in Cryptography, LNCS 7707, pp 16-33, 2013.
[3] Huang, Z. and Lin, D.: Solving polynomial systems with noise over F2: Revisited, Theoretical Computer Science, Volume 676, Page 52-78, 2017.
[4] https://magma.maths.usyd.edu.au/magma/handbook/text/1179
[5] Bard G V, Courtois N T, Jefferson C. Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over GF (2) via SAT-solvers. 2007.