第五届(2020 年)全国高校密码数学挑战赛

赛题征集通知

由教育部高等学校数学类专业教学指导委员主办、中国科学院郑志明院士发起的全国高校密码数学挑战赛已连续举办四届，共吸引了来自上百所高校的数千名学生参赛，影响范围逐年扩大。

命题工作作为本项赛事的核心，每道赛题的背后都凝聚了历届命题专家的心血，正是他们提供了高质量、高水平的赛题，让参赛选手们可以尽情发挥，为赛事的高起点、高定位奠定了基础。2019 年 8 月 8 日，在第五届（2020 年）全国高校密码数学挑战赛启动仪式上，赛事命题专家组组长、中科院信工所林东岱研究员表示新赛季命题将同时采用邀请及向全社会公开征集的方式，集思广益，力求把赛题质量提高到更高层次。现发布第五届赛题（2020 年）全国高校密码数学挑战赛命题征集方案，诚挚邀请广大科研机构、高等院校以及企业的专家学者积极参与。

一、命题范围和要求

1、命题范围

竞赛题目应是具有密码学应用背景的数学问题，在密码学中具有实际意义和应用。竞赛题目应面向普通高等院校数学系高年级学生和相关学科的研究生，并应考虑到目前教学基本内容和新技术应用趋势。

2、命题要求

赛题原则应是未被解决的密码学中的数学问题或其关联部分，既要求能让参赛人员短时间内能够上手，在短时间内能够获得成果，又能允许参赛者持续攻关，不断进展，便于优秀学生的发挥和创新。同时，命题应充分考虑到竞赛评价的操作性。

3、命题格式

（1）题目名称：要求简明扼要；

（2）赛题描述：需对题目作必要说明，明确赛题中的符号、基础知识及评分标准；

（3）密码学背景及相关问题的研究进展：命题人应对命题的意图、涉及的主要知识范围及其它问题予以必要的说明；

（4）参考文献：列出三篇涉及主要知识点的参考文献，供选手参考。

二、征题时间及内容安排

1、公开征集时间

2019 年 9 月 1 日至 2019 年 10 月 31 日。

2、提交方式

请通过电子邮件方式提交至：ddlin@iie.ac.cn

3、命题评审

命题工作组将组织专家在 2019 年 11 月 30 日之前完成对已收到赛题的初审工作，并将第一时间通知通过初审的赛题命题人，命题人根据安排参加题目修订及相关活动，并对命题内容予以保密。

4、赛题发布

赛事组委会根据命题工作组安排完成赛题的正式发布，命题专家将作为新赛季的评委参与赛事相关活动，同时在年度总决赛颁奖典礼上将获得赛事组委会颁发的“优秀命题奖”荣誉及命题奖金。

三、历届赛题

1、2016 年
赛题 1：极大布尔多项式方程组可满足性问题
赛题 2：MDS 矩阵的构造
赛题 3：RSA 加密体制破译

2、2017 年
赛题 1：布尔函数方程的求解问题
赛题 2：相关攻击中的数学问题
赛题 3：密码算法布尔函数代数次数问题
赛题 4：极大布尔多项式方程组可满足问题

3、2018 年
赛题 1：序列的有理分数表示
赛题 2：整数分解
赛题 3：离散对数求解问题
赛题 4：密码算法布尔函数代数次数问题；

4、2019 年
赛题 1：椭圆曲线离散对数问题
赛题 2：小整数解问题
赛题 3：加法链问题

有关本赛事的详细信息以及历年赛题详情可访问大赛官网 www.cmsecc.com 或关注赛事官方微信公众号（全国高校密码数学挑战赛）。

附件：第五届(2020 年)全国高校密码数学挑战赛命题模板

教育部高等学校数学类专业教学指导委员会

主任章：

二〇一九年九月