

编号：ZT-231029303

# 2023 年主题案例征集项目申报表

单位名称：南京邮电大学

首席专家：王志伟

项目名称：国产密码算法 SM9 的设计与扩展应用

填表日期：2023-12-18

教育部学位与研究生教育发展中心  
中国专业学位案例中心

## 一、基本信息

<b>(一) 项目信息</b>					
主题方向	大国智造				
项目名称	国产密码算法 SM9 的设计与扩展应用				
关 键 词	大国智造的思政元素、国产 SM9、数学基础，功能扩展				
涉及专业 学位类别	密码				
<b>(二) 首席专家信息</b>					
姓 名	王志伟	性 别	男	行政职务	无
职 称	正高级	联系电话	15951856018	电子邮箱	zhwwang @njupt.edu .cn
通讯地址	南京邮电大学计算机学院 840 信箱				
<b>(三) 团队成员信息</b> （原则上不超过 5 人，不包括首席专家）					
姓 名	性 别	职 称	工作单位及职务	联系电话	
王少辉	男	副高级		15062217110	
李琦	男	副高级		13851489961	
张平	男	中级		15751879469	
<b>(四) 预期成果形式及数量</b>					

A.教学型案例 1 个 B.研究型案例 0 篇

## 二、选题依据

简述项目的选题考虑、案例内容、学理价值、适用课程、开发计划等。（限 500-2000 字）

**【温馨提示】本项目实行同行专家通讯评议，请勿在此部分表述中透露个人信息或相关背景资料。**

为了在技术上避免受制于人，自 2010 年起，国家密码管理局陆续颁布了一系列国产密码算法，简称国密，包括国产标识算法 SM9，它也成为了 ISO/IEC 国际标准。国产密码算法的设计本身就体现了大国智造的文化自信，是融入《密码学》课程教学最好的思政元素。另一方面，虽然包括 SM9 在内的我国商用密码实现了“从无到有”的跨越式发展，但其设计初衷是满足网络与信息系统的共性基础安全需求，缺乏由其衍生的功能型密码。基于我国商用密码 SM9，开展功能型密码的研究，丰富完善我国商用密码体系是非常必要的。

标识算法设计的初衷是为了简化传统公钥密码基础设施（PKI，Public Key Infrastructure）体系中复杂公钥证书管理。这种密码算法的设计目标是让通信双方在不需要 PKI 的情况下，以实体的有效身份（如邮件地址、手机号码、QQ 号、身份证码等）作为公钥，来保证信息交换的安全性并可以验证相互之间的签名。SM9 标识密码算法包含总则、数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法、参数定义五个部分。由于涉及较多的数学基础，SM 系列国密算法只有在研究生课程《密码学》教学中才会介绍。本项目研究 SM9 国密算法的设计和扩展应用的教学过程，适用于网络空间安全专业或电子信息类研究生的《现代密码学》课程教学。

本案例的主要内容包括三个方面：课程思政元素设计，SM9 密码算法的教学设计以及 SM9 密码算法扩展的再思考设计。其中，课程思政元素从密码的红色价值观，大国智造文化自信两个维度进行设计。在 SM9 教学中融入爱国主义和民族自信心教育，有助于提高学生的文化自信和民族自豪感。SM9 密码算法教学设计应该从数学基础理论，算法流程，和安全证明的关键点三个方面进行。SM9 的数学基础理论主要是描述清楚椭圆曲线双线性映射的性质，算法流程中最关键的是深入理解密钥封装算法，而难度较大的安全性证明要基本理解其思想。SM9 密码算法的功能性扩展作为启发思考的方向，主要包括如何向多用户扩展，如何将签名和加密结合等。

本案例的教学模式设计按照问题引入、生活实例的密码方案构造、数学基础、课程思政、算法设计与证明和扩展应用顺序展开教学，难点是数学基础（数学思维训练），学习的重点是算法构造与证明、扩展应用（密码思维训练）。该模式符合方案构造的逻辑顺序，具体是第一步问题引入，即传统公钥密码体制证书管理的缺陷；第二步生活实例的密码方案构造，即用用户 Email 地址或身份证号取代公钥的可行性；第三步数学基础，即双线性配对理论；第四步课程思政，即我国自主创新的标识密码体制诞生故事；第五步 SM9 算法设计与证明；第六步 SM9 在几个方向的扩展应用。本案例设计的理论依据首先是国密 SM9 天然蕴含的思

政元素；然后是教学理论上的认知科学理论和启发式理论，激发学生独立思考的兴趣。

### 三、项目基础

简述完成项目开发的可行性，包括资料获取、相关授权、条件保障等情况；简述首席专家及团队成员承担或参与的案例项目、科研项目等的情况。（限 300-1500 字）

**【温馨提示】**本项目实行同行专家通讯评议，请勿在此部分表述中透露个人信息或相关背景资料。

《现代密码学》是网络空间安全一级学科的核心课程，在硕士和博士的培养方案中至关重要。首席专家及其团队具有较好的数论与代数基础，密码学基础，积极从事密码科学研究，掌握密码学最新的可证明安全方法和数学假设，具有爱国主义情怀和高度的文化自信，了解密码领域的中国故事。首席专家在科研过程中掌握和案例相关的国密 SM9 研究进展，包括应用范围和理论证明。首席专家长期从事从本科到博士的系列密码学课程的教学工作，做了一些探索，并取得了一些经验。首席专家所在学校在 2002 年获批信息安全本科专业，2018 年获批网络空间安全硕士点，2022 年获批网络空间安全博士点，在资料获取、相关授权、条件保障等方面都具有充分的条件。上述条件证明了本项目的可行性。

首席专家于 2009 年获得密码学博士学位，现为教授，博导。先后入选多个人才项目。先后主持完成国家自然科学基金面上项目 3 项，以及多个省部级项目和 CCF-胡杨林基金等横向项目。发表密码学方面重要期刊和会议论文 100 多篇，现为江苏省计算机学会网络与分布式计算专委会副主任，中国计算机学会分布式计算专委会委员，中国电子学会信息论分会委员，江苏省密码学会理事等。首席专家多年主讲本科，硕士，博士密码学课程，其撰写的密码教学案例入选江苏省研究生首批优质教学资源，多次获得全国密码技术竞赛优秀指导教师奖，和中国密码学会最佳教学论文奖等。

#### 四、申报承诺

我承诺对本申报表填写的各项内容的真实性和有效性负责，所填内容已征得团队成员同意，保证没有知识产权争议。若填报失实或违反有关规定，首席专家和所在单位承担全部责任。如获准立项，我承诺按照本申报项目信息表为依据，按计划认真开展研究工作，取得预期研究成果。中国专业学位案例中心有权使用本申报书所有数据和资料。

首席专家(签字)

年 月 日

#### 五、申报单位推荐意见

单位公章

年 月 日

#### 六、教育部学位与研究生教育发展中心审核意见

单位公章

年 月 日