附件 1：

“十三五”国家密码发展基金密码理论研究课题选题指南

“十三五”期间，国家密码发展基金资助密码理论研究的范围如下：

一、 密码基础理论研究

主要包括：计算数论和计算代数中的困难问题；计算复杂性理论；代码混淆理论；量子密码、混沌密码、生物密码以及其他新型密码基础理论等。

二、 密码算法设计与分析理论研究

主要包括：流密码、分组密码、杂凑密码、消息鉴别码、认证加密、公钥密码、后量子密码、全同态密码以及其他新型密码算法的自主创新设计论与分析方法；密码算法可证明安全理论；面向白盒实现的密码算法设计理论等。

三、 密码协议研究

主要包括：零知识证明协议；安全多方计算协议；身份认证与密钥交换协议；隐私保护协议；典型环境中的实用安全协议；后量子安全协议；安全协议可证明安全与形式化分析理论；量子密码协议等。

四、 密码工程与应用研究

主要包括：密码算法实现技术；侧信道攻击与防御技术；

随机数发生器原理与实现技术；密钥和密码体制安全防护技术；生物特征与密码融合的技术；密码的白盒实现技术；云计算、物联网、大数据、移动互联网、工业控制系统、数字货币中的密码应用技术；未来密码应用发展趋势等。

五、 密码系统测评分析研究

主要包括：密码算法与协议合规性测评技术；白盒密码测评理论与技术；密码模块安全测评技术；侧信道及其防御测评理论与技术；密码软件测评理论与技术；密码应用系统测评技术；量子密码安全测评理论与技术等。

六、 密码管理研究

主要包括：密码发展史；国外密码管理政策；未来密码管理政策；密码政策支撑工具；技术发展对密码管理的影响；密码监管政策对密码行业的影响以及密码标准体系建设等。