附件 1：

“十二五”国家密码发展基金密码理论研究课题选题指南

“十二五”期间，国家密码发展基金资助密码理论研究的范围如下：

一、 密码算法设计理论研究

主要包括：序列密码、分组密码、公钥密码、杂凑算法、消息认证码等算法的自主创新设计理论与技术。

二、 密码算法分析理论研究

主要包括：序列密码、分组密码、公钥密码、杂凑算法、消息认证码等算法的分析理论与技术。

三、 其他密码的设计与分析

主要包括：量子密码、抗量子计算的公钥密码、信息隐藏、混沌密码、生物密码等的设计与分析。

四、 密码协议的研究

主要包括：密码协议的可证明安全性理论、协议的形式化分析方法、面向新型应用的密码协议设计与分析等。

五、 密钥管理研究

主要包括：密钥管理理论的研究，云计算、物联网等新网络环境和新应用中的密钥管理体系等。

六、 密码实现理论与技术研究

主要包括：密码安全实现、密码高性能实现、随机数生成的理论与技术等。

七、 密码系统的测评分析理论与技术研究

主要包括：密码模块的测评理论与技术，密码系统的测评理论与技术，能量分析、电磁分析、故障注入分析等侧信道分析理论与技术。

八、 密码管理相关问题研究

主要包括：密码管理、标准、专利及其他问题的分析及对策研究。

九、 其他与密码理论研究相关的方面，如与密码理论相关的数学问题、应急与灾备的密码理论。