**附件1：**

**“十三五”国家密码发展基金密码理论研究课题**

**2018年度选题指南**

“十三五”国家密码发展基金2018年立项资助密码理论研究的范围如下：

 **1.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；代码混淆理论等。

 **2.密码算法设计与分析**

主要包括：对称密码和公钥密码的自主创新设计与分析；量子计算密码分析；白盒密码算法设计与实现技术等。

 **3.密码协议研究**

研究形成密码协议设计与分析的理论、方法和平台，主要包括：密码协议基本模块、安全模型和归约方法、可证明安全与形式化分析理论；针对新应用的典型环境中的实用安全协议；量子密码协议等。

 **4.密码工程技术研究**

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等。

 **5.密码系统测评分析研究**

主要包括：密码标准符合性测评技术；白盒密码测评理论与技术；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等。