终端密码协同安全计算关键技术及其应用

（技术发明奖）

一、推荐意见

专家推荐意见1（北京信息科学技术研究院 蔡吉人）

全面推广密码应用是一项重要的国家战略。亿级用户终端上的合规安全密码部署是我国商用密码应用推进的重要环节，也是促进关键信息基础设施和重要信息系统全面部署密码应用的关键。现有用户终端来源复杂、平台差异大、运行环境不受控，安全合规的密码部署技术难度大。

该项目提出了协同密码计算方案，支持在终端以软件形式安全实现密码计算，有效克服了安全与易部署、高效之间的矛盾，并通过高质量随机数生成和高性能协同密码服务等体系化创新，成果推广取得显著成效。

项目成果得到产业和应用的使用验证，推动了我国软件密码产业生态的形成和发展，受到国家密码主管部门的高度认可和肯定。

推荐为中国科学院杰出科技成就奖（技术发明奖）候选者。

专家推荐意见2（网络空间部队信息工程大学 郑建华）

构筑商用密码网络安全保障体系是我国的重大战略。长期以来，我国关键基础设施和重要互联网应用都使用外挂式专用密码硬件形式部署，存在成本高、管理困难、便捷性差等问题。

项目发明了一种终端软件与远端密码服务器协同的安全密码计算方案；基于时间分片的终端密码安全计算技术；浮点定点协同的服务端高性能密码技术；软件随机数生成及评估方法，形成了适应各在用终端部署的体系化密码技术方案。

项目成果得到密码主管部门的肯定，获得了显著的经济效益，并在国家基础设施、电子政务外网等重要领域得到应用。

特推荐为中国科学院杰出科技成就奖（技术发明奖）候选者。

专家推荐意见3（复旦大学 柴洪峰）

在全国范围用户终端上部署合规的标准密码算法对于全面推进我国商用密码应用意义重大。该项目在国家密码主管部门的指导下，完成了具有我国特色的软件密码技术创新发明，突破了我国商用密码应用推进面临的技术难题，有显著的应用价值。

项目基于风险分散的技术思想，设计了椭圆曲线密码协同算法和协议，完成了密钥随机数生成、高性能协同密码计算服务器等体系化技术发明，推动构建了具有我国特色的软件密码技术体系。

项目完成了包括技术发明、产品研发、标准编制、应用推广等在内全链条发明创新，形成规模化应用，取得了显著的经济效益和社会效益，得到国家密码主管部门的高度认可和肯定。

特推荐为中国科学院杰出科技成就奖（技术发明奖）候选者。

专家推荐意见 4（空军研究院 王建华）

互联网关键信息系统需要终端大范围部署安全合规的密码算法软硬件。开放环境中的移动终端平台差异化大，推广专用密码硬件成本高、部署难度大。该项目面向这一国家需求，开展技术攻关。

项目基于门限密码原理，面向我国标准算法，发明了椭圆曲线密码协同计算方法，实现了相关终端密码产品。相对国际基于同态的协同密码方案，性能大幅提升，达到了实用化要求。项目还完成了密钥随机数生成、高性能协同密码服务器等技术研发，完善了技术链。

项目成果得到规模化推广，并在可信身份、电子政务等重要领域得到应用，经济和社会效益显著，获得党政机要密码科学技术一等奖。

特推荐为中国科学院杰出科技成就奖（技术发明奖）候选者。

专家推荐意见 5（合肥国家实验室 何良生）

无需终端专用硬件的软件密码技术，对在我国用户终端中大范围部署合规安全的密码，服务百姓网络信息安全，推广我国密码应用，具有重大意义。

现有用户终端运行环境复杂，如何保障密码计算安全是亟待破解的技术难题。该项目发明了协同密码计算方法，可将远程可信密码计算安全引入终端密码软件，通过安全协作实现开放终端上的安全密码计算。该发明充分利用我国椭圆曲线密码算法自身的计算特点，在不引入同态密码等其他额外数学安全基础的条件下，实现更加高效的密

码计算安全协同。

项目在密钥安全、高性能协同服务器等配套技术方面开展了体系化创新，并开展了规模化推广，经济社会效益显著。

推荐为中国科学院杰出科技成就奖（技术发明奖）候选者。

二、主要发明专利列表

序号	发明专利名称	国家（地区）	授权号	授权日期	发明人	发明专利有效状态
1	一种抗能量分析攻击的基于SM2算法的两方协同签名方法	中国	ZL2020 11156120.2	2023年6月27日	荆继武;尤玮婧;王平建;刘丽敏;王跃武;雷灵光;寇春静	有效
2	一种基于SM2密码算法的高效门限签名方法	中国	ZL2021 11153521.7	2023年7月04日	荆继武; 张译尹; 王平建; 王跃武; 雷灵光; 刘丽敏; 寇春静; 孙思维; 王　鹏;杨峰	有效
3	一种保护用户隐私的盲协同签名方法	中国	ZL2021 11466500.0	2023年12月19日	荆继武; 王平建; 王跃武; 王　鹏; 雷灵光; 刘丽敏; 孙思维; 寇春静	有效
4	一种将特定数值作为分享份	中国	ZL2020 10920060.0	2023年6月27日	荆继武;何俊霖;王平建;寇春静	有效

	额的秘密分享方法					
5	一种保护用户隐私的 SM2 密码算法协同签名、解密方法	中国	ZL2021 11465919.4	2025 年 6 月 10 日	荆继武;王平建;王跃武;王鹏;雷灵光;刘丽敏;孙思维;寇春静	有效
6	一种多个节点链式协作签名的方法	中国	ZL 2022 11115672.8	2025 年 8 月 12 日	王平建;荆继武;王跃武;王鹏;雷灵光;刘丽敏;孙思维;寇春静	有效
7	Key protecting method and apparatus	欧洲	EP3113 406B1	2020 年 4 月 29 日	林璟锵;管乐;王琼霄;汪婧;荆继武	有效
8	一种基于双内存异或的加密计算机系统及总线加密方法	中国	ZL2023 10310260.8	2025 年 6 月 17 日	荆继武;张子昂;王跃武;郭润;寇春静	有效
9	一种寄存器内完成连续矩阵乘法的计算方法及装置	中国	ZL2024 10273106.2	2024 年 10 月 11 日	郑昉昱;周天;荆继武;王跃武;林璟锵;孙思维;边毅	有效
10	一种实现素数域大整数模乘计算加速的方法	中国	ZL2021 10783676.2	2024 年 6 月 25 日	郑昉昱;高莉莉;魏荣;马　原;王跃武;范广;万立鹏	有效

三、其他知识产权和标准等列表

序号	类型	名称	著录信息	全部完成人
1	标准	《网络安全技术 基于密码令牌的主叫用户可信身份鉴别技术规范》	国家标准 GB/T 43779-2024	荆继武；王跃武；刘紫千；上官晓丽；刘丽敏；魏亮；詹榜华；寇春静；任兰芳；郑学欣；王平建；颜雪薇；常新苗；雷灵光；黄钱红；李根；王榕；王鹏；华孝泉；吴越；鲍博武；陈木来；梁宁宁；吴昊；李彦峰；王志辉；胡建勋；金刚；张宇；吕召彪；李俊；刘为华；廖正赟；周蔚林；罗影；张文科；吴强；陈晶；赵文博
2	标准	《软件随机数发生器设计指南》	密码行业标准 GM/T 0105-2021	马原；吕娜；陈华；沈海斌；郑昉昱；陈天宇；张翌维；樊俊锋；林璟锵；刘攀；吴鑫莹；张立廷；吴震；王飞宇；张文婧；胡晓波；范丽敏；韩玮
3	论文专著	Cache-in-the-Middle (CITM) Attacks: Manipulating Sensitive Data in Isolated Execution Environments	2020 ACM SIGSAC Conference on Computer and Communications Security,（ACM CCS， CCF A，信息安全类顶会）	Jie Wang(王跃武的博士研究生); Kun Sun; Lingguang Lei; Shengye Wan; Yuewu Wang; Jiwu Jing
4	论文专著	On the Analysis and Improvement of Min-Entropy Estimation on Time-Varying Data	IEEE Transactions on Information Forensics and Security，vol. 15, pp. 1696 - 1708, 2020（TIFS， CCF A，信息安全类	Shuangyi Zhu; Yuan Ma（通讯作者）; Xusheng Li; Jing Yang; Jingqiang Lin; Jiwu Jing

			顶刊）	
5	论文专著	DPF-ECC: A Framework for Efficient ECC with Double Precision Floating-Point Computing Power	IEEE Transactions on Information Forensics and Security，vol. 16, pp. 3988 - 4002, 2021（TIFS， CCF A，信息安全类顶刊）	Lili Gao（王跃武的博士研究生）; Fangyu Zheng（通讯作者）; Rong Wei; Jiankuo Dong; Niall Emmart; Yuan Ma; Jingqiang Lin; Charles Weems

四、成员贡献情况

排序	姓名	工作单位	主要贡献
1	荆继武	中国科学院大学	提出了椭圆曲线密码拆分和协同签名技术路线，给出了基于通用器件的密钥保护思路，完成了高性能密码安全实现技术的总体设计，构建了足熵随机数发生器设计模型。对应技术发明点（1）、（2）、（3）。
2	王跃武	中国科学院大学	负责技术方案研究和关键技术突破，为密钥拆分软件和协同签名软件密码技术设计了具体的密码协议和实现方案，提出了基于通用计算平台的密码计算隔离技术思路。对应技术发明点（1）、（2）。
3	马原	中国科学院信息工程研究所	负责随机数质量保障方面的研究工作，提出软件随机数熵估计方法，编制了软件随机数发生器设计的国家密码行业标准。对应技术发明点（1）、（3）。
4	林璟锵	中国科学技术	负责协同签名软件密码技术的原型系统实现工作，提出并实现了利

		大学	用通用计算平台硬件事物内存的密码计算隔离方案，开展了密码高性能密码技术在重点领域的推广应用。对应技术发明点（2）、（3）。
5	郑昉昱	中国科学院大学	负责高性能密码技术实现，发明了浮点-定点混合高性能密码实现技术，设计了安全的高性能密码设备整体结构，完成了高性能安全密码设备的研制。对应技术发明点（3）。
6	王平建	中国科学院信息工程研究所	负责协同签名软件的架构设计和实现关键技术研究，提出了基于门限的协同签名的实现技术及优化方案，参与完成了协同签名的标准化。对应技术发明点（1）。

说明：公示内容须与推荐书相关部分一致。