协同签名及其安全保障技术

（技术发明奖）

（中国科学院大学）

1、 推荐意见（不超过300字）

面对我国密码产业发展中面临的终端安全问题，提出了基于门限的密码协同签名技术，通过将密码签名计算拆分到终端和服务器两方，有效降低了因终端丢失、病毒或系统破解等带来的安全风险，开辟了具有我国特色的密码安全计算新模式。

围绕协同签名方案的实施，发明了基于时间分片的终端密码安全计算技术；发明了浮点定点协同的服务端高性能密码技术；提出了软件随机数生成及评估方法；确保了协同签名体系实用化。

协同签名及安全保障技术，开创了我国密码软件产业新形态，带动相关销售超27亿元。在国家身份基础设施、电子政务外网等重要领域得到广泛应用。

该技术曾获得2022年度密码科学技术一等奖。

推荐为中国科学院杰出科技成就奖（技术发明奖）候选者。

2、 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	ZL202011156120.2	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	ZL202111153521.7	2023 年 07 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	一种适用于门限计算的 SM2 数字签名方法	中国	ZL202010919794.7	2023 年 10 月 13	荆继武；张译尹；王平建；刘丽敏；寇春静	有效
4	一种保护用户隐私的盲协同签名方法	中国	ZL202111466500.0	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

5	一种将特定数值作为分享份额的秘密分享方法	中国	ZL202010920060.0	2023 年 06 月 27 日	荆继武；何俊霖；王平建；寇春静	有效
6	一种可信的敏感数据保护方法及系统	中国	ZL201910073175.8	2021 年 7 月 13 日	荆继武；王跃武；雷灵光；周　荃；李彦初；马　超；王　杰；林璟锵	有效
7	一种轻量级可信通道及其通信控制方法	中国	ZL202111202062.7	2023 年 08 月 15 日	雷灵光；王跃武；周　荃；史昊天；王　杰；寇春静	有效
8	一种针对内核数据的容器安全加固系统及方法	中国	ZL202111144132.8	2023 年 10 月 03 日	雷灵光；王跃武；周　荃；许守银；王平建；寇春静	有效
9	一种利用 AI 加速器实现环上多项式乘法计算加速的方法和装置	中国	ZL202010498697.5	2023 年 09 月 26 日	郑昉昱；万立鹏；林璟锵	有效
10	一种实现素数域大整数模乘计算加速的方法	中国	ZL202110783676.2	2024 年 06 月 25 日	郑昉昱；高莉莉；魏　荣；马　原；王跃武；范　广；万立鹏	有效

3、 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	《信息安全技术 基于多信道的证书申请和应用协议》	国家标准 GB/T 40018-2021	牛莹姣（荆继武的博士研究生）；荆继武；高　能；陈　星；刘丽敏；汪宗斌；贾世杰；雷灵光；杨　楠；郑昉昱；马　原；王平建；吕　娜；钱文飞；张永强；王天华；林雪焰
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	学术论文	Vulnerable Service Invocation and Countermeasures	IEEE Transactions on Dependable and Secure Computing，vol. 18, no. 4, pp. 1733-1750, 1 July-Aug. 2021 （TDSC， CCF A，信息安全类）	Huan Chang（荆继武的博士研究生）； Lingguang Lei（通讯作者）； Kun Sun; Yuewu Wang; Jiwu Jing;

				Yi He; Pingjian Wang
4	学术论文	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
5	学术论文	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）	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

4、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，给出了基于隔离计算技术的密钥保护思路，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）、（4）。
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	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）。
4	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）。
5	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（4）。
6	雷灵光	中国科学院信息工程研究所	负责基于通用计算部件的协同签名软件的安全防护机制设计和实现，设计了协同签名模块访问控制隔离机制，完成了软件密码计算隔离机制的具体方案设计和实现。对应技术发明点（2）。