浙江省科学技术奖公示信息表（单位提名）

提名奖项：科学技术进步奖

|  |  |
| --- | --- |
| 成果名称 | 数据要素密态计算关键技术及应用 |
| 提名等级 | 一等奖 |
| 提名书相关内容（附表） | 附表 |
| 主要完成人 | 任奎，排名1，正高，浙江大学韦韬，排名2，正高，支付宝（杭州）信息技术有限公司王磊，排名3，高级工程师，浙江蚂蚁密算科技有限公司马晓航，排名4，浙江网商银行股份有限公司陈文智，排名5，正高，浙江大学朱国平，排名6，高级工程师，中电云计算技术有限公司闫守孟，排名7，无，浙江蚂蚁密算科技有限公司秦湛，排名8，正高，浙江大学李婷婷，排名9，无，浙江蚂蚁密算科技有限公司王志波，排名10，正高，浙江大学张秉晟，排名11，正高，浙江大学张园超，排名12，无，浙江网商银行股份有限公司袁伟斌，排名13，无，中电云计算技术有限公司 |
| 主要完成单位 | 1.支付宝（杭州）信息技术有限公司2.浙江大学3.浙江蚂蚁密算科技有限公司4.浙江网商银行股份有限公司5.中电云计算技术有限公司 |
| 提名单位 | 浙江省数字经济联合会 |
| 提名意见 | 项目围绕高性能密态计算平台核心技术体系，聚焦可信软硬件底座、高性能计算框架、高通用密态大模型等密态计算关键技术，开展技术攻关，研发形成了密态计算通用平台，项目技术创新显著，并在实际业务场景下进行了广泛应用。主要技术创新点如下：1.研发了可信根芯片Blade-T、可信执行环境HyperEnclave、可信操作系统0cclum全栈技术，构建了首个国产自主可控的密态计算软硬件体系，摆脱了对CPU可信根的依赖。2.研发了高性能的可信隐私保护计算框架“隐语”，建立了低延时、高并发、强扩展的密态数据分析处理环境，大幅提高了密码协议的性能，突破了大规模数据密态计算应用落地关键技术。3.研发了国内首个密态大模型训练和推理平台，通过MPC协议优化和高效近似计算技术，显著降低了密态大模型推理过程中的通信开销，实现了从密态数据处理到大模型推理的全链路打通。项目构建了高效、安全、可控的密态计算平台，技术难度大、创新性强、应用面广，整体技术达到国际先进水平，其中密态计算软硬件底座、密态计算框架及算子库、密态大模型计算平台达到国际领先水平。项目已成功应用于金融、医疗、农业等国计民生行业，服务超亿级用户，累计新增经济效益超40亿元。 |

主要知识产权和标准规范目录

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 知识产权（标准规范）类别 | 知识产权（标准规范）具体名称 | 国家（地区） | 授权号（标准规范编号） | 授权（标准发布）日期 | 证书编号（标准规范批准发布部门） | 权利人（标准规范起草单位） | 发明人（标准规范起草人） | 发明专利（标准规范）有效状态 |
| 发明专利 | 一种可信应用的运行方法，装置及设备 | 中国 | ZL202010231197.5 | 2022/12/27 | 第5343258号 | 支付宝（杭州）信息技术有限公司 | 秦凯伦；刘双；顾宗敏；闫守孟 | 授权 |
| 发明专利 | 分布式多方安全计算系统，方法和节点 | 中国 | ZL202111608228.5 | 2022/05/06 | 第5137247号 | 支付宝（杭州）信息技术有限公司 | 潘无穷；李婷婷；韦韬；张煜龙；段然；钱中天；李天 | 授权 |
| 发明专利 | SECURE MULTI-PARTY COMPUTATION METHODS AND APPARATUSES | 英国 | EP 4262134 B | 2024/10/30 | EP4262134 B | 支付宝（杭州）信息技术有限公司 | 陆宇飞；王磊；张磊；崔锦铭 | 授权 |
| 发明专利 | 一种支持可组合SQL查询的加密数据库方法 | 中国 | ZL02110886135.2 | 2023/9/29 | 第6370506号 | 浙江大学 | 刘健；曹新乐；芦浩；任奎 | 授权 |
| 发明专利 | 一种基于模型分割的大模型隐私保护推理方法 | 中国 | ZL202311418709.9 | 2024/04/05 | 第6874195号 | 浙江大学 | 乔一帆；邵硕；秦湛；王志波；任奎 | 授权 |
| 发明专利 | 一种基于大数据的高可信度学习资源安全共享方法及装置 | 中国 | ZL202411038288.1 | 2024/11/26 | 第7559630号 | 浙江大学 | 赵均益；刘金飞；文龙；任奎 | 授权 |

代表性论文专著目录

|  |  |  |  |
| --- | --- | --- | --- |
| 作 者 | 论文专著名称/刊物 | 年卷页码 | 发表时间（年、月） |
| Zhenyang Dai, Shuang Liu, Vilhelm Sjoberg, Xupeng Li, Yu Chen, Wenhao Wang, Yuekai Jia, Sean Noble Anderson, Laila Elbeheiry, Shubham Sondhi, Yu Zhang, Zhaozhong Ni, Shoumeng Yan, Ronghui Gu, Zhengyu He | Verifying Rust Implementation of Page Tables in a Software Enclave Hypervisor/ ACM International Conference on Architectural Support for Programming Languages and Operating Systems（ASPLOS） | 2024,2: 1218-1232 | 2024.4 |
| Yibiao Lu, Bingsheng Zhang, Kui Ren | Low Communication Secure Computation From Semi-Trusted Hardware/IEEE Transactions on Information Forensics and Security（TIFS） | 2023, 18: 3962-3976 | 2023.1 |
| Junming Ma, Yancheng Zheng, Jun Feng, Derun Zhao, Haoqi Wu, Wenjing Fang, Jin Tan, Chaofan Yu, Benyu Zhang, and Lei Wang | SecretFlow-SPU: A Performant and User-Friendly Framework for Privacy-Preserving Machine Learning/USENIX Annual Technical Conference（USENIX ATC） | 2023, 17-33 | 2023.7 |
| Wen-jie Lu, Zhicong Huang, Zhen Gu, Jingyu Li, Jian Liu, Cheng Hong, Kui Ren, Tao Wei, Wenguang Chen | BumbleBee: Secure Two-party Inference Framework for Large Transformers/Network and Distributed System Security Symposium（NDSS） | 2025, 1-18 | 2025.2 |