2025年度福建省科学技术奖拟提名项目公示内容

高校：南京航天航空大学

项目名称：面向数据要素安全共享的关键密码构造理论与方法

提名奖种：自然科学奖

提名单位：福建省教育厅

项目简介：

随着数据作为战略资源地位凸显，如何实现数据资源安全共享、充分释放数据要素价值，已成为数据要素市场化配置的核心问题。密码技术是保障网络与信息安全的核心支撑，然而，传统密码技术难以抵御密态数据搜索所面临的令牌伪造、陷门延展等多维攻击，无法满足密态数据可控共享对发送方隐私保护、权限高效撤销等复合需求，亦难以应对数据认证中安全分析支撑不足、管控机制缺失等现实挑战，在安全性、功能性和实用性三个层面均亟待突破。项目面向数据要素国家战略需求，在国家优青、国家优青（海外）、教育部“长江学者奖励计划”（青年学者）、国家自然科学基金重点项目、福建省引才“百人计划”/杰青/重点项目等项目支持下，针对密态数据可信搜索、可控共享、可验认证等关键需求，系统性提升了密码方案的安全强度，丰富了密码构造的功能体系，优化了密码算法的执行效率，为数据要素安全流通、高效配置与价值实现提供了坚实的理论与方法支撑。项目的主要科学发现如下：

1、面向复杂攻击的数据要素“可信搜索”强安全密码新机制：提出了可搜索加密的科学分类体系和形式化建模方法，构建了面向复杂攻击的密态搜索安全性科学评估理论，所提评估方法准确率约为 CCS 2016 经典方法的881倍，为复杂攻击场景下密态搜索的安全可信运行提供了关键评估支撑（代表性论文1、2）；

2、面向复合需求的数据要素“可控共享”多功能密码新方法：定义了属性基匹配加密新型密码原语，提出了支持细粒度“双向访问控制”多类型专用功能的密态数据共享构造理论与技术体系，提升了密码技术对多元复合需求的支撑能力，为复杂需求场景下密态数据可控共享提供了理论与技术支撑（代表性论文3）；

3、面向复杂环境的数据要素“可验认证”高实用密码新构造：证明了SM9数字签名算法满足EUF-CMIA安全性，改进SM9密钥封装算法并提出了高实用性方案Twin-SM9，给出了基于无中心变色龙哈希与BLS短签名的可验认证通用构造方法，为自主可控的高实用国产密码研究提供了理论与构造支撑（代表性论文4、5）。

项目培养1名国家杰青、1名国家优青、1名国家优青（海外）、1名教育部青年长江学者和1名国家重点研发计划项目首席科学家。5篇代表性论文，谷歌学术引用368次，SCI他引161次，CNKI他引54次，欧洲科学院院士、加拿大皇家学会院士、ACM SIGSAC杰出贡献奖获得者等同行广泛引用和高度评价了项目所提出的理论与方法。项目完成人获2018年

教育部自然科学奖一等奖、2023年教育部自然科学二等奖、2022年中国密码学会密码创新奖一等奖、2023年中国密码学会优秀青年奖、第25届欧洲计算机安全学术会议最佳论文奖（国内唯一），担任中国密码学会常务理事、亚密会指导委员会委员（三位国内代表之一）、CCF A类期刊编委，连续多年入选科睿唯安全球高被引学者、爱思唯尔中国高被引学者，主持完成国家自然科学基金重点项目、优青和优青（海外）项目各1项。

主要完成单位：

福建师范大学

主要完成人及其贡献：

黄欣沂：项目总负责人和设计者，带领项目组系统开展相关密码理论与方法研究。主要学术贡献为：提出了密态数据搜索的分类体系；提出了面向多类型专用功能的密态数据共享构造理论；证明了SM9数字签名算法满足EUF-CMIA安全性，并提出了Twin-SM9算法。是代表性论文1、2、3和5的通讯作者，对科学发现一、二、三都做出了重要贡献。（自2012年2月至2023年3月在福建师范大学工作，2023年4月离职）

宁建廷：主要学术贡献为：设计了可搜索加密的形式化建模方法，提出了加密网络流隐私保护安全计算构造理论，构建了密态搜索安全性科学评估理论；定义了属性基匹配加密密码原语，构建了支持多功能密态数据安全共享构造方法；提出了面向可修订区块链“修订次数可控”的设计思想，实

现了区块链修订权限的可控认证。是代表性论文1和2的第一作者，代表性论文3的合作者，代表性论文4的通信作者，对科学发现一、二、三做出了重要贡献。

代表性论文专著目录：

1. 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS 2021)、LEAP: Leakage-Abuse Attack on Efficiently Deployable, Efficiently Searchable Encryption with Partially Known Dataset、0.000、2021 年 2307-2320、2021 年 11 月 13 日、EI 收录、12 次、作者：1/Jianting Ning (宁建廷)、2/Xinyi Huang (黄欣沂/通讯作者)、3/Geong Sen Poh、4/Jiaming Yuan (袁家明)、5/Yingjiu Li、6/Jian Weng (翁健)、7/Robert H. Deng；

2. 2020 European Symposium on Research in Computer Security (ESORICS 2020)、Pine: Enabling Privacy-Preserving Deep Packet Inspection on TLS with Rule-Hiding and Fast Connection Establishment、0.000、2020 年 3-22、2020 年 9 月 12 日、EI 收录、13 次、作者：1/Jianting Ning (宁建廷)、2/Xinyi Huang (黄欣沂/通讯作者)、3/Geong Sen Poh、4/Shengmin Xu (许胜民)、5/Jia-Chng Loh、6/Jian Weng (翁健)、7/Robert H. Deng；

3. IEEE Transactions on Dependable and Secure Computing、Match in my way: Fine-Grained Bilateral Access Control for Secure Cloud-Fog Computing、7.300、2022 年第 19 卷 1064-1077、2020 年 9 月 12 日、SCI/EI 收录、82 次、作者：1/Shengmin Xu (许胜民)、2/Jianting Ning (宁建廷)、3/Yingjiu Li、4/Yinghui Zhang

(张应辉)、5/Guowen Xu (徐国文)、6/Xinyi Huang (黄欣沂/通讯作者)、7/Robert H. Deng；

4. IEEE Transactions on Information Forensics and Security、K-Time Modifiable and Epoch-Based Redactable Blockchain 、7.231、2021 年第 16 卷 4507-4520、2021 年 8 月 24 日、SCI/EI 收录、54 次、作者：1/Shengmin Xu (许胜民)、2/Jianting Ning (宁建廷/通讯作者)、3/Jinhua Ma (马金花)、4/Xinyi Huang (黄欣沂)、5/Robert H. Deng；

5. 中国科学:信息科学、国密 SM9 数字签名和密钥封装算法的安全性分析、0.000、2021 年第 51 卷 1900-1913、2021 年 11 月 4 日、CSCD 收录、54 次、作者：1/赖建昌、2/黄欣沂 (通讯作者)、3/何德彪、4/伍玮。

其他支撑材料目录：

1.任务来源

(1) 国家自然科学基金委、否、同态数据认证（国家自然科学基金优青项目）、61822202；

(2) 国家教育部、否、教育部“长江学者奖励计划”青年学者项目、无；

(3) 国家自然科学基金委、否、数据安全（国家自然科学基金优青（海外）项目）、F22E001K912B08；

(4) 国家自然科学基金委、否、公共平台中个人健康记录的安全保障技术研究（国家自然科学基金面上项目）、61472083；

(5) 国家自然科学基金委、否、云环境下安全数据共享与访问控制机制研究（国家自然科学基金面上项目）、61972094；

(6) 福建省科技厅、否、福建省引才“百人计划”（创新人才）项目、ZAC1700107。

2. **曾获科技奖励情况**

(1) 匿名多因素身份认证理论与方法、2018-02-27、教育部自然科学奖、一等奖、国家部委、中国人民解放军设立的科学技术奖；

(2) 数字签名的多功能融合原理与设计方法、2023-06-06、教育部自然科学奖、二等奖、国家部委、中国人民解放军设立的科学技术奖；

(3) 中国密码学会密码创新奖一等奖、2022-12-09、中国密码学会密码创新奖、一等奖、经登记的社会力量设立的科学技术奖；

(4) 中国密码学会优秀青年奖、2023-12-08、中国密码学会优秀青年奖、其他、经登记的社会力量设立的科学技术奖；

(5) Pine: Enabling privacy-preserving deep packet inspection on TLS with rule-hiding and fast connection establishment 、2020-09-14、ESORICS 最佳论文奖、其他、国际组织和外国政府设立的科学技术奖。

3．**其他证明**

(1) 计划任务书或合同书、任务委托书等、公钥密码学（国家自然科学基金杰青项目）资助项目计划书首页、国家自然科学基金委；

(2) 计划任务书或合同书、任务委托书等、基于我国商用密码的区块链安全保护研究（国家自然科学基金重点项目）资

助项目计划书首页、国家自然科学基金委；

(3) 计划任务书或合同书、任务委托书等、云数据安全分享技术（福建省自然科学基金杰青项目）任务书和结题证明、福建省科技厅；

(4) 计划任务书或合同书、任务委托书等、同态数字签名的理论与设计（福建省自然科学基金重点项目）任务书和结题证明、福建省科技厅；

(5) 其他相关资料、福建省“闽江学者奖励计划”特聘教授、福建省教育厅；

(6) 其他相关资料、福建省级高层次B类人才、福建省委人才工作领导小组办公室；

(7) 其他相关资料、蚂蚁隐语-优秀产学合作贡献奖、蚂蚁隐语开源社区；

(8) 其他相关资料、福建省计算机学会2024年学术年会论文一等奖、福建省计算机学会；

(9) 检索查新报告、科技查新报告、科学技术部西南信息中心查新中心；

(10) 检索查新报告、代表性论文检索报告、科学技术部西南信息中心查新中心；

(11) 其他相关资料、黄欣沂福建师范大学工作证明、福建师范大学人事处；

(12) 其他相关资料、知情同意证明(代表性论文3、4)、福建师范大学计算机与网络空间安全学院；

(13) 其他相关资料、知情同意证明(代表性论文5)、福建

师范大学计算机与网络空间安全学院；

(14) 其他相关资料、谷歌学术引用次数证明、福建师范大学计算机与网络空间安全学院。