

项目情况简介（省自然科学奖）

1、项目名称

数据要素全生命周期安全的关键密码理论

2、主要完成人

张应辉，郑东

3、提名单位

陕西省教育厅

4、提名意见

该项目属于密码学与数据安全研究领域。项目组围绕数据要素在全生命周期中所面临的安全威胁与隐私泄漏风险展开深入研究，突破了数据采集与传输过程的跨域可信安全、数据存储与共享过程的细粒度匿名可控性以及数据使用与销毁过程的安全计算与可验证性等理论难题，为构建数据要素全生命周期安全保障体系奠定了关键理论基础。

针对数据采集与传输过程，创建了安全高效的跨域数据源可靠性保障方法，为数据安全传输协议的设计与安全性分析开辟了新途径。针对数据存储与共享过程，实现了存储过程中无需任何第三方的远程数据完整性校验，引入细粒度解密测试的思想克服了用户隐私保护需求与移动性数据访问之间的矛盾。针对数据使用与销毁过程，克服了密文检索中用户和服务方的双向验证以及外包计算结果的正确性验证等理论挑战，去除了安全数据删除必须依赖于第三方可信中心的信任假设。项目成果被包括科学院和工程院院士、IEEE (Life) Fellow、ACM Fellow、IACR Fellow 在内的中、美、英、法、德等世界各国学者广泛引用和积极评价，被作为基本理论框架用于设计云计算、车载自组网、外包计算和公平支付等应用场景的安全解决方案。符合陕西省自然科学奖二等奖推荐条件。

推荐该项目为陕西省自然科学奖二等奖。

5、项目简介

该项目属于密码学与数据安全研究领域。项目组围绕数据要素在全生命周期中所面临的安全威胁与隐私泄漏风险开展研究，主要成果如下：

1、创建了安全高效的跨域数据源可靠性保障方法，克服了数据采集安全必须依赖于可信第三方的理论挑战，创新性地将变色龙哈希函数引入到安全协议的

设计中，为数据安全传输协议的设计与安全性分析开辟了新途径。

2、实现了数据在存储过程中无需任何第三方的远程完整性校验，给出了数据存储安全算法的系统性安全与性能评估标准，引入细粒度解密测试的思想克服了数据共享所面临的用户隐私保护需求与移动性数据访问之间的矛盾。

3、克服了密文检索和外包计算结果正确性难以验证的理论挑战，突破了数据删除无法验证的理论难点，去除了安全数据删除必须依赖于第三方可信中心的信任假设。

6、客观评价

项目成果荣获陕西省自然科学优秀学术论文一等奖 1 项，陕西高等学校科学技术研究优秀成果一等奖 1 项。来自中国、美国、英国、德国、加拿大、澳大利亚、瑞典等世界各地的高校包括各个国家科学院院士、工程院院士和 IEEE (Life) Fellow、ACM Fellow、IACR Fellow 在内的知名专家，在 IEEE TIFS、Science China Information Sciences、ACM CCS 等期刊和会议上发表论文对相关成果给予肯定性评价。相关成果被来自世界各地的知名科研团队广泛采用，包括在信息系统著作《Information Systems Outsourcing-The Era of Digital Transformation》和国际密码学、安全和隐私百科全书《Encyclopedia of Cryptography, Security and Privacy》等著作中介绍或收录，被作为基本理论框架用于设计云计算、车载自组网、外包计算和公平支付等应用场景的安全解决方案。

7、代表性论文专著目录

序号	论文专著名称	刊名	作者	年卷页码(XX年 XX 卷 XX 页)	发表时间	通讯作者	第一作者	国内作者	SCI他引总次数	知识产权是否归国内所有
1	Robust and universal seamless handover authentication in 5G HetNets	IEEE Transactions on Dependable and Secure Computing	Yinghui Zhang* , Robert H. Deng, Bertino Elisa, Dong Zheng	2021 年 18 卷 2 期 858-874 页	2021 年 03 月 12 日	Yinghui Zhang	Yinghui Zhang	张应辉, 郑东	87	是
2	Attribute-based encryption for cloud computing access control: a survey	ACM Computing Surveys	Yinghui Zhang* , Robert H. Deng, Shengmin Xu, Jianfei Sun, Qi Li, Dong Zheng	2020 年 53 卷 4 期 83 号论文 1-41 页	2020-08-01	Yinghui Zhang	Yinghui Zhang	张应辉, 李琦, 郑东	111	是
3	Security and privacy in smart health: efficient policy-hiding	IEEE Internet of Things Journal	Yinghui Zhang* , Dong Zheng , Robert	2018 年 5 卷 3 期 2130-2145 页	2018-06-08	Yinghui Zhang	Yinghui Zhang	张应辉, 郑东	330	是

	attribute-based access control		H. Deng							
4	Blockchain based efficient and robust fair payment for outsourcing services in cloud computing	Information Sciences	Yinghui Zhang* , Robert H. Deng, Ximeng Liu, Dong Zheng	2018 年 462 卷 262-277 页	2018-06-15	Yinghui Zhang	Yinghui Zhang	张应辉, 郑东	145	是
5	Outsourcing service fair payment based on blockchain and its applications in cloud computing	IEEE Transactions on Services Computing	Yinghui Zhang* , Robert H. Deng, Ximeng Liu, Dong Zheng*	2021 年 14 卷 4 期 1152-1166 页	2021-08-05	Yinghui Zhang, Dong Zheng	Yinghui Zhang	张应辉, 郑东	91	是
合 计									764	

8、主要完成人情况

排序	完成人	行政职务	技术职称	工作单位	完成单位	对本项目的贡献
1	张应辉	科研处副处长	教授	西安邮电大学	西安邮电大学	作为项目负责人，对项目的研究进行总体规划，负责项目技术路线的制定和具体实施。是三个创新点的第一完成人（见代表性论文 1-5）。
2	郑东	陕西密码工程研究院院长	教授	西安邮电大学	西安邮电大学	作为项目第二完成人，参与了数据源安全认证、数据安全传输、匿名校验和访问控制，以及安全计算与可验证机制的研究，是三个创新点的第二完成人（见代表性论文 1-5）。

9、主要完成单位情况

排序	完成单位	对本项目的贡献
1	西安邮电大学	作为本项目的负责单位，西安邮电大学为项目的顺利完成做出了重要贡献，主要表现为：（1）组织并完成了项目策划和实施工作；（2）为项目的顺利实施提供了人力资源与优质的工作环境与场所；（3）提供了本项目所需的图书资料和数据库等资源；（4）依托我校无线网络安全技术国家工程研究中心等优势平台始终大力支持项目负责人的科研工作。

10、完成人合作关系说明

项目负责人张应辉和第二完成人郑东目前是同事且同属于西安邮电大学无线网络安全技术国家工程研究中心课题组，合作发表论文并获批知识产权、共同获奖、共同承担科研项目，并取得丰硕的研究成果。代表性论文 1-5 均由张应辉和郑东合作发表。