**公示信息**

青海省2021年度科技进步奖：

一、项目名称：通用可复合密码协议研究

二、提名单位：青海师范大学

三、提名意见：该项目由西安邮电大学联合青海师范大学、格尔软件股份有限公司，依托国家自然科学基金委地区项目和青海省基础研究计划项目，推进产学研用协同创新与技术攻关，取得以下科技创新成果：

（1）通用可复合安全的身份代理签密协议、自认证盲签密协议和ElGamal型广播多重签密协议，这些协议实现了复杂的网络环境下保密并认证的消息传输，可以根据实际需求用于电子投票、电子支付、电子拍卖等领域。

（2）通用可复合安全的身份混合签密协议、采用双线性对的无证书混合签密协议和无证书椭圆曲线混合签密协议的签密KEM和DEM各自独立，安全性可以分开研究，非常适合用在复杂的网络环境中需要签密任意长度消息的场景。

（3）通用可复合安全的群签名协议和群盲签名协议，可以保证与多个协议并发执行时的安全以及作为复合协议组件时的安全，协议中群成员可以代表群针对消息进行签名，验证者使用群公钥可以对签名进行验证，发生争议时群管理员可以追踪到签名者的身份。

该项目的通用可复合密码技术应用到了格尔软件股份有限公司的数字证书系统和安全认证网关系统中。该项目创新产品全国销售100多个单位和企业，近三年的新增利润累计133,94.64万元，其中2018年新增利润3632.43万元，2019年为3843.08万元，2020年为5919.13万元。

四、主要知识产权目录

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **授权项目名称** | **知识产权类别** | **授权国家** | **授权号** | **授权日期** | **权利人** | **发明人** | **有效状态** |
| 1 | 通用可复合的身份代理签密方法 | 发明专利 | 中国 | ZL201811210167.5 | 2019-10-25 | 西安邮电大学青海师范大学 | 俞惠芳, 王之仓 | 有效 |
| 2 | 无证书环境下椭圆曲线盲签密方法 | 发明专利 | 中国 | ZL201811210151.4 | 2019-10-29 | 西安邮电大学青海师范大学 | 俞惠芳, 王之仓 | 有效 |
| 3 | 基于乘法群的无证书环签密方法 | 发明专利 | 中国 | ZL201911212292.4 | 2020-11-20 | 西安邮电大学 | 王之仓, 俞惠芳 | 有效 |
| 4 | 无证书环境下具有强指定验证者的多变量多重签名方法 | 发明专利 | 中国 | ZL202010114481.4 | 2020-11-20 | 西安邮电大学 | 王之仓, 俞惠芳 | 有效 |
| 5 | 从证书公钥系统到身份公钥系统的匿名签密方法 | 发明专利 | 中国 | ZL201310740351.1 | 2017-02-01 | 西安邮电大学 | 张应辉, 郑东, 赵庆兰, 任方 | 有效 |
| 6 | 从身份公钥系统到证书公钥系统的匿名签密方法 | 发明专利 | 中国 | ZL201310740804.0 | 2017-01-25 | 西安邮电大学 | 张应辉, 郑东, 赵庆兰, 任方 | 有效 |
| 7 | 一种基于身份且签名长度恒定的在线离线聚合签名方法 | 发明专利 | 中国 | ZL201710226131.5 | 2020-06-30 | 西安邮电大学 | 张应辉, 闫铭, 郑东, 吕柳迪, 苏昊楠 | 有效 |
| 8 | 一种支持系统属性扩展的属性基加密系统及方法 | 发明专利 | 中国 | ZL201510249462.1 | 2018-05-18 | 西安邮电大学 | 张应辉, 郑东, 赖成喆 | 有效 |
| 9 | 基于AMI和5G智能电网下电力注入的隐私保护方法 | 发明专利 | 中国 | ZL201611156134.8 | 2020-10-20 | 西安邮电大学 | 张应辉, 邓恺鑫, 郑东, 赵江凡, 吴阿新 | 有效 |
| 10 | 基于区块链的数据完整性验证方法、设备和存储介质 | 发明专利 | 中国 | ZL201910329009.X | 2021-05-04 | 西安邮电大学 | [张应辉,](https://cprs.patentstar.com.cn/Search/ResultList?CurrentQuery=5byg5bqU6L6JL0lO&type=Cn) [徐永庆,](https://cprs.patentstar.com.cn/Search/ResultList?CurrentQuery=5b6Q5rC45bqGL0lO&type=Cn) [吴阿新,](https://cprs.patentstar.com.cn/Search/ResultList?CurrentQuery=5ZC06Zi/5pawL0lO&type=Cn) [张甜甜,](https://cprs.patentstar.com.cn/Search/ResultList?CurrentQuery=5byg55Sc55ScL0lO&type=Cn) [邹健,](https://cprs.patentstar.com.cn/Search/ResultList?CurrentQuery=6YK55YGlL0lO&type=Cn) [郭瑞,](https://cprs.patentstar.com.cn/Search/ResultList?CurrentQuery=6YOt55GeL0lO&type=Cn) [郑东](https://cprs.patentstar.com.cn/Search/ResultList?CurrentQuery=6YOR5LicL0lO&type=Cn) | 有效 |

五、主要完成人情况

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **排序** | **完成人** | **技术职称** | **工作****单位** | **完成****单位** | **对本项目的贡献** |
| 1 | 俞惠芳 | 教授 | 西安邮电大学 | 西安邮电大学 | 项目总负责人，负责制定国家自然科学基金地区项目和青海省基础研究计划项目的总体的研究方案、技术路线和实施计划，具体创造性贡献体现在通用可复合密码协议的具体实例的设计工作，设计出的协议实例的正确性分析、安全性证明和性能评估的工作，两个已授权中国发明专利的文案工作，由科学出版社出版的专著《混合签密理论》的撰写和校对工作。 |
| 2 | 赵 峰 | 教授 | 西安邮电大学 | 西安邮电大学 | 具体的创造性贡献体现在负责该项目科技成果推广及应用工作，针对无证书椭圆曲线混合签密的协议实例的形式化的算法定义工作，相应的协议实例的正确性分析工作和性能评估的仿真实验工作，为解决通用可复合密码协议的量子计算问题提供新的思路和方法的抗量子计算协议的设计工作。 |
| 3 | 王之仓 | 教授 | 西安邮电大学 | 西安邮电大学 | 具体的创造性贡献体现在通用可复合的采用双线性对的无证书混合签密和无证书椭圆曲线混合签密的协议实例的形式化的安全模型构造工作，相应协议实例的性能评估工作，两个已授权中国发明专利的文案工作，专著《混合签密理论》的校对工作。 |
| 4 | 孟 茹 | 研究员 | 格尔软件股份有限公司 | 格尔软件股份有限公司 | 具体的创造性贡献体现在：代表格尔软件股份有限公司对技术开发（委托）合同的接洽工作，同时负责格尔软件股份有限公司针对技术的实施和落实情况的文案工作。 |
| 5 | 张应辉 | 教授 | 西安邮电大学 | 西安邮电大学 | 具体的创造性贡献体现在从证书公钥系统到身份公钥系统的匿名签密方法、从身份公钥系统到证书公钥系统的匿名签密方法、基于身份的密钥长度恒定的在线离线聚合签名方法等六个授权中国发明专利的文案工作。 |
| 6 | 李建民 | 助理工程师 | 青海省气象局 | 青海师范大学 | 李建民是项目申请人俞惠芳在2015年9月至2018年7月指导的硕士研究生。其创造性贡献体现在通用可复合安全的ElGamal型多重签密协议以及自认证盲签密协议的形式化的安全模型构造工作，协议实例的设计和正确性分析工作，相应协议实例的安全性证明部分工作和性能评估工作。 |
| 7 | 赵 晨 | 无 | 北京得到信息科技有限公司 | 青海师范大学 | 赵晨是项目申请人俞惠芳在2014年9月至2017年7月指导的硕士研究生。其创造性贡献体现在通用可复合群签名和群盲签名协议的算法定义和安全模型工作，相应具体实例的设计和正确性分析工作、设计出的协议实例的通用可复合安全性证明以及性能评估工作。 |

六、主要完成单位及创新推广贡献

|  |  |  |
| --- | --- | --- |
| **排序** | **完成单位** | **对本项目的贡献** |
| 1 | 西安邮电大学 | 西安邮电大学是工业和信息化部与陕西省共建，国家在西北地区部署的唯一通信类高等学校。针对单个协议与多个协议并发执行或作为复合系统组件时无法保证安全的问题，西安邮电大学联合青海师范大学、格尔软件股份有限公司经过多年艰苦攻关取得以下创新成果：（1）提出通用可复合的基于身份的代理签密协议，使代理签密者通过获得原始签密者委托授权，对指定的消息进行代理签密；如果发生否认争议，指定的接收者能宣布任何第三方对密文进行验证，无需额外计算工作。通过基于身份的代理签密协议的理想功能，说明了该密码协议与自适应选择密文攻击下的不可区分性和自适应选择消息下的不可伪造性之间存在等价关系。（2）出版专著《混合签密理论》，该书说明混合签密由非对称签密密钥封装机制和对称数据封装机制组成，能实现任意长度消息的保密并认证的安全通信，非对称部分和对称部分的安全需求完全独立，这两部分安全性（含通用可复合安全性）完全可以分开研究，这使之在密码学安全应用中具有更高的灵活性。该书旨在深入理解和掌握混合签密协议的设计理念，对网络空间安全、信息安全、信息对抗、网络工程等专业的本科生、研究生的学习具有很好的指导作用和参考价值。技术成果（1）作为专著《可证明安全签密理论》的重要内容之一，目前该书在校样并由《科学出版社》待出版。累计培养信息安全方向硕士研究生26名。 |
| 2 | 青海师范大学 | 青海师范大学已有65年的历史，现有教职工1290人，拥有博士学位授权点，是一所综合性、高水平的师范大学。为了推进青海信息安全发展，青海师范大学经过多年艰苦攻关取得以下技术创新成果：（1）通用可复合的自认证盲签密和ElGamal型广播多重签密的算法简单、通信开销低、安全性高、鲁棒性强，可以实现复杂网络环境下的保密并认证的消息传输。（2）通用可复合的基于身份的混合签密、采用双线性对的无证书混合签密和无证书椭圆曲线混合签密，适合用在需要签密任意长度消息的网络环境中。（3）通用可复合的群签名可以广泛应用于电子选举、电子投标、电子现金系统领域。通用可复合的群盲签名能实现验证者使用群公钥对签名进行验证，发生签名争议时仅有群管理员可以追踪到签名者的身份，在群成员代表群进行消息签名但不允许知道所签消息内容的情形下非常实用。研究成果系统化了的通用可复合安全的密码协议的理论体系，推动了通用可复合密码协议研究的整体发展，提升了青海省乃至我国通用可复合密码协议的整体研究水平和发展空间。累计培养信息安全方向硕士研究生4名。成果（1）涉及到的两个密码协议作为专著《可证明安全签密理论》的两个重要内容。 |
| 3 | 格尔软件股份有限公司 | 格尔软件股份有限公司是国内首批研制和推出公钥基础设施产品的厂商，在密码研究和应用领域处于国内领先地位。曾获国家科技进步二等奖2项、上海科技进步一等奖1项、党政密码科学进步一等奖1项、国家教育部科技进步二等奖1项。格尔软件股份有限公司经过多年的理论研究和技术实践，取得以下应用成果：格尔数字证书认证系统和格尔安全认证网关已经过大规模的商业化检验，广泛应用于交通、电力以及工控等领域。加速推进了金融、政务和商务等领域的密码产品国产化替换进程，密码技术产品得到创新研发，提升了产业安全，提高了国产密码产业支撑能力，扩大了国产密码产品应用范围，推动了密码与行业深度融合，构建了完备的密码产品体系，打造了密码产业生态，构建了现代国产化密码体系，提升了密码供给质量。积极布局前沿技术以及密码技术的协同创新，加强关键信息基础设施密码保障体系，构建以密码技术为核心的关键信息基础设施安全保障体系。落实国家密码应用政策和密码法要求，引领信息领域关键核心技术的突破，构建以密码为基石的网络空间新安全，将密码融入网络架构，构建新网络安全体系，建设新网络安全环境，保障网络安全。西安邮电大学、青海师范大学和格尔软件股份有限公司三方合作，实现了企业、高校和科研院所等产学研主体的深度融合。以重大科技项目为纽带，以产学研联盟为载体，突破了一批共性技术和关键核心技术，促进了产业结构转型升级，构建了协同创新治理机制。 |