陕西省科学技术进步奖提名书

（2023年度）

一、项目基本情况

项目名称	开放环境下数据安全共享与处理关键技术研究与应用
主要完成人	杨晓元，王绪安，周潭平，韩益亮，汤殿华，李朋林，刘振华，吴立强，刘龙飞
主要完成单位	中国人民武装警察部队工程大学 中国电子科技集团公司第三十研究所 上海同态信息科技有限责任公司 西安电子科技大学

二、提名意见（适用于部门、机构提名）

提 名 者	中国人民武装警察部队工程大学	提名等级	□一等奖 √二等奖及以上□三等奖及以上

提名意见：

开放环境下数据安全共享与处理关键技术研究与应用项目，受到多项国家重点研发计划项目、国家自然科学基金项目、陕西省自然科学基金项目等的资助，针对学科前沿和现实应用需求，为破解“数据孤岛问题”展开研究，取得了良好的研究成果。突出性的成果包括攻破了 IEEE P1363.3 草案中的重要方案、提出了发方代理重加密的密码学原语、丰富了现有多密钥全同态加密的密文扩展形式。项目形成的相关成果在陕西空港自贸产业发展有限公司、西安中拓明光科技有限公司的密态计算系统及安全数据计算与应用平台、中国电子科技集团第三十所相关信息系统中得到应用，且产生了可观的社会效益和经济效益。

说明：省科学技术奖一、二、三等奖项目，实行按等级标准提名、独立评审表决的机制。提名单者应严格依据省科学技术奖的标准条件，说明提名项目的贡献程度及等级建议。“仅提名一等奖”评审落选项目不再降格参评二等奖，“提名二等奖及以上”的评审落选项目不再降格参评三等奖。提名项目正式提交后，提名等级建议本年度不得变更。

二、提名意见（适用于专家提名）

姓　　名			
专家类型	□国家最高科学技术奖获得者 □中国科学院院士 □中国工程院院士 □国家科学技术奖获奖项目第一完成人（需注明获奖等次） □省最高科学技术奖获奖人（或 xxxx 年省科学技术最高成就奖、xxxx 年基础研究重大贡献奖获奖人） □Xxxx 年省科学技术奖第一完成人（需注明获奖等次）	提名等级	□一等奖□二等奖及以上□三等奖及以上
责任专家	□是　　□否		
提名意见： 说明：省科学技术奖一、二、三等奖项目，实行按等级标准提名、独立评审表决的机制。提名单者应严格依据省科学技术奖的标准条件，说明提名项目的贡献程度及等级建议。“仅提名一等奖”评审落选项目不再降格参评二等奖，“提名二等奖及以上”的评审落选项目不再降格参评三等奖。提名项目正式提交后，提名等级建议本年度不得变更。			

三、项目简介

随着云计算和人工智能等技术的迅猛发展，大量的数据被生成、收集和存储。产业界和民众对数据安全和个人隐私的重视和担忧，导致大量数据不再愿意被共享，从而形成“数据孤岛”的困境。因此，对开放环境下数据安全共享与处理关键技术进行研究与应用具有重要价值。本项目在国家重点研发计划项目、国家自然科学基金项目、陕西省自然科学基金项目等多项基金支持下取得丰硕成果，发表相关论文 50 余篇，其中 SCI 检索 20 余篇，授权相关发明专利 5 项，申请相关发明专利 10 余项，获得多项软件著作权，参与制定多项行业标准及发布行业报告，如《云计算中同态加密技术应用要求》《金融场景的隐私保护计算平台技术要求与测试方法》《数字生态银行场景安全研究报告（2022 版）》《数据要素安全流通白皮书》等，在国内外形成了一定的影响力和示范效应。代表性成果如下：

（1）提出了多项基于代理重加密的开放环境下数据安全共享技术

代理重加密的概念由 Blaze 等人在 Eurocrypt98 上提出，如图 1 所示，其核心思想是使用代理 P 将发送给 A（被代理者）的密文转化为 B(代理者)可以利用其私钥解开的密文，但在这个转化过程中要求代理不能得知被转化密文所对应的明文，也不能得知 A 和 B 的私钥。

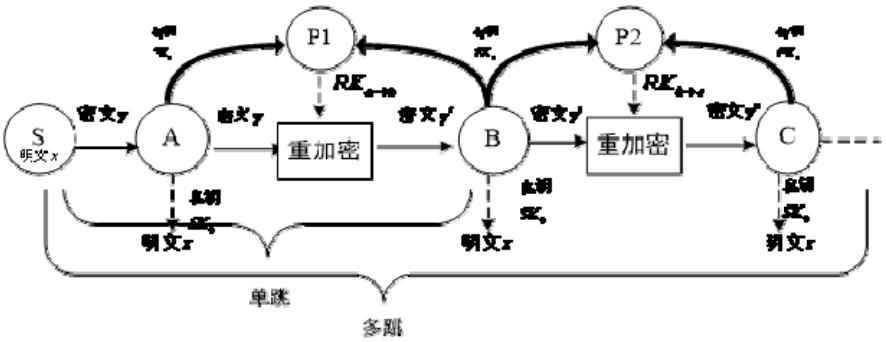

图 1　代理重加密示意图

基于代理重加密的开放环境下数据安全共享技术，围绕代理重加密多样化设计与分析作出了如下研究工作：

①分析了日本 NTT DATA 公司提交给 IEEE P1363 公钥密码标准化组的基于双线性配对的基于身份的代理重加密提案，指出该方案是不安全的，从而导致该提案被从 IEEE P1363.3 草案中删除，受到 IEEEP1363 公钥密码标准化组的较高评价并开辟网页介绍该成果，如图 2 所示，提高了我国在该提案方面的话语权。

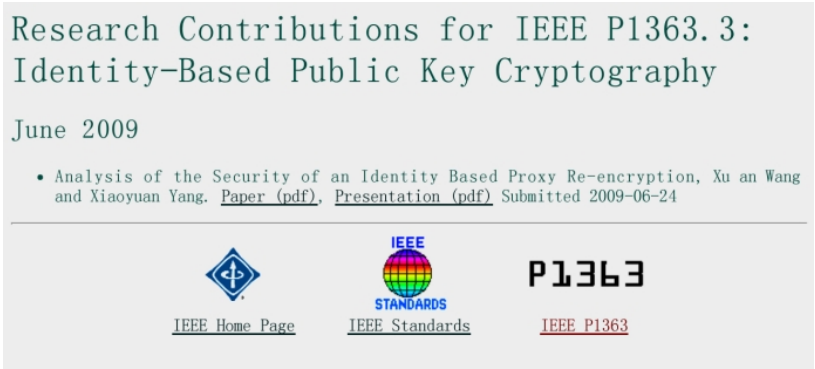

图 2　项目组对基于双线性配对的基于身份代理重加密提案的研究贡献

②提出了发方代理重加密的概念，其模型示意图如图 3 所示，这种新型代理重加密体制可以看作是传统代理重加密体制的对称面。在传统代理重加密体制中由被代理者 A 来控制代理的过程，其决定了是否让 B 获知发送者 S 所发送的消息，在多跳的环境中，B 又决定是否让 C 获知发送者 S 所发送的消息，依此类推。在新型代理重加密体制中，由发送者 S 来控制代理的过程，其决定了是否让 B（单跳的环境）或者 C 及其后续的代理者（多跳的环境）获知发送者 S 发送的消息，这种新型代理重加密体制能够避免传统代理重加密体制所固有的缺点，此时发送者拥有对发送消息的获知范围的可控性，所有的接收者都没有能力生成新的代理重加密密钥。我们构造了基于离散对数困难问题的发方代理重加密方案，并探讨了该新型密码学原语在组播

密钥分配中的应用。

③设计了支持多关键字检索的代理重加密方案并探索了其在云存储中的应用。早期带关键字检索的代理重加密仅仅支持单关键字检索，并且代理能够重加密所有的第二层密文（初始密文），我们提出了单跳支持多关键字检索的单向代理重加密的概念，给出了其定义，具体方案并证明了其安全性，相关论文得到同行较好评价，在 WOS 中被引 35 次。

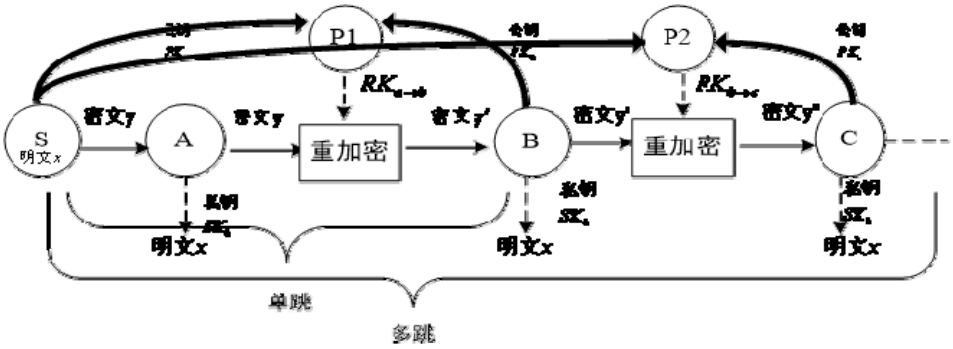

图 3　发方代理重加密示意图

④设计了多个基于格的具有附加性质的代理重加密方案，包括基于格的多跳单向基于身份的代理重加密方案，基于理想格的鲁棒门限代理重加密方案，格上抗合谋攻击的代理重加密方案，全同态代理重加密方案等。在后量子时代典型的备选密码体制中，格密码具有快速易实现、安全证明可靠、构造能力强等优势，因此以格为构造工具构造代理重加密方案对于抵抗量子计算机的威胁，实现后量子时代的密码安全具有重要意义，此外，项目组还提出了鲁棒门限代理重加密等新概念，该新概念扩展了代理重加密在密文访问控制方面的能力，如表 1 所示：

表 1 基于代理重加密方法的密文访问控制机制演化过程

代表性关键技术	驱动力	方法	服务器模型
加密和授权	数据加密且可共享	数据加密存储+授权密钥访问	完全可信
代理重加密	授权服务器权限过大、单点失败	数据公钥加密+代理执行转发	半可信
门限代理重加密	代理服务器可用性差、安全性弱、效率低	数据公钥加密+代理分散转发+合法性验证	无需可信

（2）提出了多项基于多密钥全同态等技术的开放环境下数据安全处理技术

多密钥全同态加密技术可以保证在开放环境下对不同用户的数据进行安全处理，可为云计算、人工智能等多用户参与的领域提供数据存储、传输和计算安全。认证技术是保证信息安全的基础技术，可以保证系统资源和数据仅被授权的用户进行操作。基于多密钥全同态加密和认证技术的开放环境下数据安全处理，围绕多密钥全同态加密和认证技术的设计方面作出了如下研究工作：①构建了 BGV 型多密钥全同态加密方案的密文扩展形式。早期多密钥全同态加密方案的密文扩展形式为级联式密文扩展，我们设计了嵌套式 BGV 密文扩展算法，可以将密文规模大约降低一半。目前，该技术已经成为多密钥全同态加密方案中的密文扩展的通用方式。②设计了一个具有常数签名长度的环签名方案。在数据完整性认证方面，使用多线性映射设计了一个具有常数签名长度的环签名方案。在标准模型下，基于多线性计算性 Diffie-Hellman 困难问题假设，该方案被证明抵抗完全密钥泄露是匿名安全的，抵抗选择子环攻击是不可伪造的。进一步地，该方案使用最优安全规约技术具有紧安全规约的优点。③提出了一种支持批量审计的高效无证书指定审计者云数据完整性审计方案。方案利用动态哈希表数据结构对云端数据进行高效地更新，能够抵抗不诚实云端的伪造攻击，安全性较高，审计效率高。④提出了基于账号隐匿的第三方有效身份托管敏捷认证访问方法。通过搭建第三方身份认证服务平台，以“态安全”APP 为用户操作载体，建立统一的多因素交互身份认证接口并提供给所有公司开放使用，对接入公司进行身份认证服务并将用户认证结果以可证明的形式提供给接入公司的三方有效身份托管敏捷认证访问方法。这些研究成果发表于国内外权威期刊，得到了同行较好评价。由项目研究单位上海同态信息科技有限责任公司牵头编制的《云计算中同态加密技术应用要求》团体标准，也已经通过上海市商用密码行业协会正式发布，对国内同态加密技术的发展具有推广示范作用。

四、客观评价

“开放环境下数据安全共享与处理关键技术研究与应用”成果的相关评价如下：

①在对 IEEE P1363 公钥标准工作组的 IEEE P1363.3 草案的标准化工作方面，我们主要是对日本 NTT DATA（三菱数据公司）密码学者 Matsuo 提交给 IEEE P1363 标准工作组关于代理重加密的草案进行了密码学分析，我们将这一研究工作提交给 IEEE P1363 标准化工作组，得到了其高度评价，开辟网页专门介绍了该研究工作，见图 2，这直接导致日本 NTT DATA（三菱数据公司）提交的关于代理重加密的草案被从 P1363.3 草案中删除(目前 P1363.3 标准化提案已经成熟并发布，不再包含代理重加密标准化方案部分)。

②在发方代理重加密（PRE+）方面，目前该密码学原语已经获得国际同行的一定关注，且评价较高。2020 年，本领域信息安全类 SCI 检索期刊 Journal of Information Security and Applications（CCF C 类期刊）上发表论文 Provably secure lattice based identity based unidirectional PRE and PRE+ schemes，对 PRE+进行了跟踪研究，该论文评价我们的 PRE+工作如下：In 2013, Wang et al. introduced a new primitive: PRE+, which is similar to the conventional PRE except that, in PRE+ scheme encryptor computes re-encryption keys. Here encryptor is the delegator.We have also constructed a lattice identity based unidirectional PRE+ scheme(2013 年，王等人首次引入一个新的密码学原语：PRE+。该密码学原语与传统的代理重加密（PRE）基本相似，除了在 PRE+中由加密者计算重加密密钥。在 PRE+中,加密者就是授权人，我们也构造了一个基于格的单向发方代理重加密方案)。该文同时对基于身份的 PRE+ 的定义，安全模型，格构造等给出了详细的描述。2020 年，本领域综合类 SCI 期刊 Computer Communications 上发表论文 GROSE: Optimal group size estimation for broadcast proxy re-encryption，也对 PRE+给出了较高评价：Wang et al introduced an IPR plus scheme, where the re-encryption keys are encrypted by the encryptor instead of the delegator. Here the encryptor can decide who can act as the proxy server(王等人首次引入了发方代理重加密的密码学原语，其代理重加密密钥由加密者而不是授权解密者生成。此处加密者而不是由解密方决定谁将担任代理服务器的角色)。其它还有一些论文引用或借鉴了 PRE+的相关工作，在此不赘述。

③在支持多关键字检索的代理重加密方案，我们的研究工作也获得了较高评价，GOOGLE 引用率达到 70，WOS 数据库中引用率达到 35。2016 年，本领域权威期刊 IEEE Transactions on Information Forensics and Security 上发表论文 Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds，对我们研究工作作出了评价： Later, Wang et al. has suggested an improved scheme to support the conjunctive keyword search function（王等人提出了一个支持多关键字搜索的改进型代理重加密方案）。2018 年，本领域权威期刊 IEEE Transactions on Services Computing 上发表论文 Searchable Encryption for Healthcare Clouds: A Survey，对我们的研究工作给出了较高评价：Wang et al. (WHY+) further extended PRES by introducing a new primitive: constrained single-hop unidirectional proxy re-encryption supporting conjunctive keywords search (CPRE-CKS)（王等人扩展了带关键字搜索的代理重加密通过引入一个新的密码学原语：支持多关键字搜索限制性的单跳单向代理重加密）。

④在基于格的后量子安全的代理重加密方案上，我们的研究成果也取得了较好的评价。发表在电子学报上的论文基于理想格的鲁棒门限代理重加密方案，审稿人认为：“该文利用理想格上工具构造了一种门限代理重加密方案，采用格上同态签名技术完成密文份额合法性的可公开验证，实现鲁棒性。在证明方法上，分析了 PRE 和 TPRE 安全模型之间的差异，然后基于游戏跳转证明方法，证明对 TPRE 的攻击可多项式时间内转化为对潜在 PRE 方案的攻击。最后给出了两种典型的应用场景。该文采用同态签名实现鲁棒性是该文的创新所在，最后的应用场景是该文的亮点。最终方案可完全抗量子攻击，是该文的优势所在。对代理重加密的研究具有借鉴作用。”。在代理重加密在云存储密文访问控制方面，发表在计算机应用上的论文基于代理重加密的云存储密文访问控制方案得到国内该领域资深学者张玉清教授等发表在软件学报上的论文《云计算环境安全综述》的较高评价：“2014 年提出的一种新型代理重加密算法解决了一对多的云存储访问控制问题. 仅将部分密文存储于云服务器，使数据发送方可以控制密文的传递范围，并降低了通信过程中的数据计算量和交换量。”

⑤在多密钥全同态加密方案的设计方面上，我们的研究工作也获得了较高评价，GOOGLE 引用率达到 25。2019 年，信息安全顶会 CCS19 上，CDKS 论文 6 次引用了我们的工作，借鉴我们的思想，对论文评价如下：This approach is similar to a method proposed in previous work [41] which also generates a shared evaluation key”“ The main technical contribution is to propose new relinearization algorithms achieving better performance compared to prior works [41]（本文工作借鉴了李等人生成共享计算密钥的方法；对比李等人的工作，本论文的主要贡献是提出了一个新的重线性化算法，提升了方案效率）。 2021 年，在计算机类 TOP 期刊 ACM Computing Surveys 中，论文 4 次引用我们的工作，给出进行评价：Li et al. [66] proposed an alternative design for MKBGV scheme that reduced the size of extended ciphertexts roughly by half（李等人提出了一种新的设计可以将扩展密文的规模降低大约一半）。

五、应用情况

1.产业应用

本项目形成的相关成果在陕西空港自贸产业发展有限公司、西安中拓明光科技有限公司的密态计算系统及安全数据计算与应用平台、中国电子科技集团公司第三十所相关信息系统等得到应用，且产生了可观的社会效益和经济效益。

相关密态计算系统已交付数据匿踪求交系统、数据沙箱、隐私协议集合等的数据共享与可信交付系统4套，隐私计算一体机8台，提供数据质量评估67次、运营服务7次、技术开发服务12次，近三年累计销售收入400多万元。

基于高效同态加密方案的安全数据计算与应用平台，实现加密数据的贝叶斯检测等共享应用，进行了药物风险性与治愈率的差异性研究，有效提高了研究命中率，降低了研究周期和成本开销。累计交付同态隐私安全网关40台、同态隐私计算一体机12台、可信共享与密文交付平台系统4套，近三年累计销售收入700多万元，取得了良好的经济效益和社会效益。

项目形成的相关成果还在中国电子科技集团公司第三十所相关信息系统等得到应用，产生了可观的社会效益和经济效益。

2.理论应用

本项目相关理论研究成果发表在国际国内权威期刊且被引用次数较高，也申请了相关专利与软件著作权，应用较为广泛，尤其是发方代理重加密和多密钥全同态加密具有较好的应用，主要应用场景包括云安全数据共享和组播密钥分配、广播加密、数据密态处理等。

首先阐述云安全数据共享方面的应用，如图5所示。数据属主Alice首先加密自己的数据，当数据用户Bob想访问Alice的数据时，代理对Alice外包的密文数据进行重加密，在这个过程中，代理不知道任何数据内容，它也不能得到Alice和Bob的任何私钥信息。传统的代理重重加密也能做这项工作，但使用发方代理重加密则可以很好的支持共享授权不可转移性和消息级别的细粒度访问控制。在传统代理重加密中，代理和Bob串通后可以代表Alice 给任意其它用户授权。显然，这违背了Alice共享数据给Bob的初衷。而使用发方代理重加密，Alice 可以很容易地控制将哪些数据内容重加密，且能支持消息级别的细粒度授权。

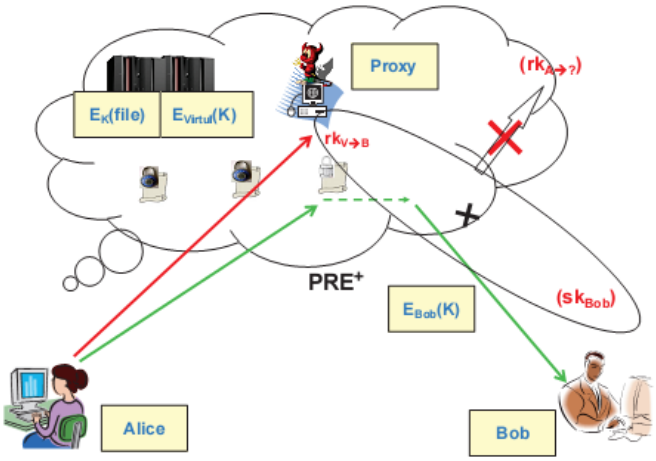

图5 云数据安全共享方面的应用

再阐述组播密钥分配方面的应用，如图6所示。多跳代理重加密，十分好的切合了安全组播密钥分配的功能需求。比如，在安全组播密钥分配中，网络拓扑结构会包含有不少的辅助节点或密文转发节点（如路由器），而这些节点正好可以被用来充当代理重加密中的代理，且无需这些节点的强可信性，只需其半可信即可。另一方面，多跳代理重加密中的代理密钥的设置也很符合动态的组播密钥分配环境，当有用户加入、退出时，只需要变更此用户附近的代理重密钥即可，无需对整个密钥分配系统作大的调整。且发方代理重加密中密钥发送方可以直接决定后续节点的密钥可授权性，更加贴合实际需求。

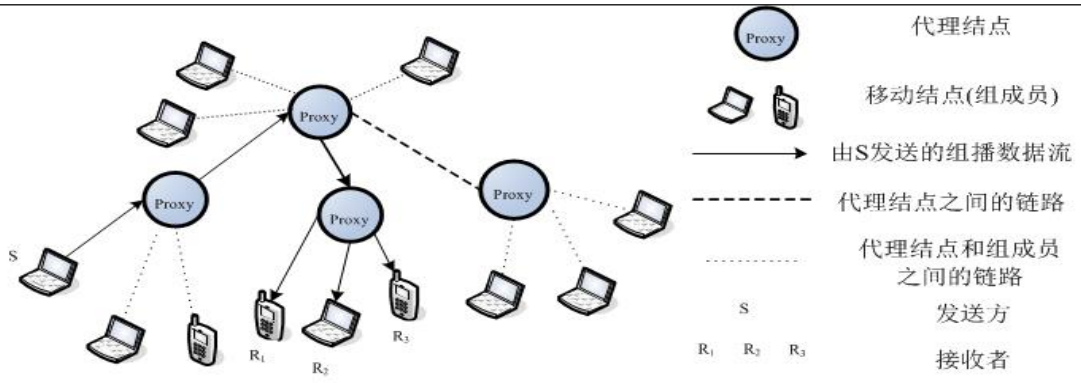

图6 组播密钥分配方面的应用

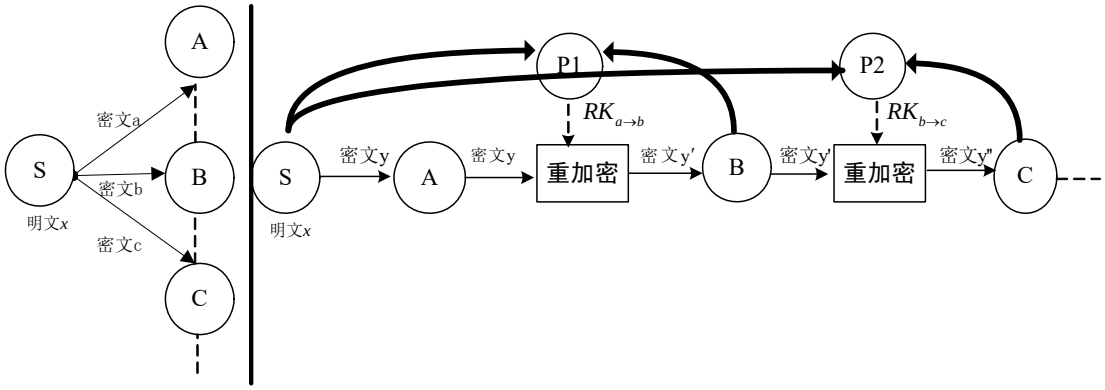

图 7　广播加密与发方代理加密对比图

再阐述在广播加密方面的应用，如图7所示。发方代理加密体制与广播加密体制也有相同点，比如，它们都很好地适应了一个发送方对多个接收者传输加密消息的场合，但它们也有较大的区别。目前来说，大多数的基于公钥的非平凡构造的广播加密具有以下这些特点：①要么密文和公开参数（不包括接收者的公钥）数量为$O(\sqrt{n})$量级；②要么密文数量为$O(1)$量级，公开参数为$O(n)$量级；③要么公开参数数量为$O(1)$量级，密文数量为$O(n)$量级，此处n指合法用户数的个数。而一旦有用户退出或加入，发送者必须重新计算整个密文，其可扩展性有限。而在基于发方代理加密体制的一对多密文传输系统中，公开参数可以独立于合法用户数量，为$O(1)$量级，密文的数量也始终是$O(1)$量级，且其可扩展性也较好。

最后阐述在密态计算方面的应用。多密钥全同态加密技术可以应用于多方参与的密态计算，基于BGV型多密钥全同态加密方案相对于早期的多密钥全同态加密方案，可以将密钥规模降低一半，有效降低多方参与用户的通信开销。

六、主要知识产权和标准规范等目录（限 10 条）

序号	知识产权类别	知识产权具体名称	国家（地区）	授权号	授权日期	证书编号	权利人	发明人
1	发明专利	组播通信用代理重加密方法	中国	ZL201310647075.4	2018-04-24	2900105	中国人民武装警察部队工程大学	王绪安，韩益亮，孟艺超，杨晓元，张敏情
2	发明专利	一种 BGV 型多密钥全同态加密方法	中国	ZL201910065976.X	2022-04-15	5083281	中国人民武装警察部队工程大学	李宁波，周潭平，杨晓元，魏立线，韩益亮，刘龙飞，吴立强，刘文超，涂广升
3	发明专利	具有快速同态运算过程 NTRU 型多密钥全同态加密方法	中国	ZL201910066014.6	2022-04-15	5419653	中国人民武装警察部队工程大学	车小亮，李宁波，周潭平，张敏情，韩益亮，刘龙飞，涂广升，刘文超
4	发明专利	基于账号隐匿的第三方有效身份托管敏捷认证访问方法	中国	ZL201811003238.4	2021-03-16	4304531	上海同态信息科技有限责任公司	李朋林，屈玮华，朱静熹，王浩
5	发明专利	一种基于揭序加密的多数据类型密文比较方法	中国	ZL202110644822.3	2022-7-05	5286101	中国电子科技集团公司第三十研究所	汤殿华，黄云帆，赵伟，任娟，尉小鹏，李泓泉
6	论文	New identity based proxy re-encryption scheme from lattices	中国	China Communication	2019-10-01	10.23919/JCC.2019.10.011	中国人民武装警察部队工程大学	吴立强，杨晓元，张敏情，刘龙飞
7	论文	基于理想格的鲁棒门限代理重加密方案	中国	电子学报	2020-09-01	10.3969/j.issn.0372-2112.2020.09.017	中国人民武装警察部队工程大学	吴立强， 韩益亮， 杨晓元， 张敏情， 杨凯
8	论文	Efficient certificateless public integrity	中国	Journal of King Saud University - Computer	2022-11-01	10.1016/j.jksuci.202	中国人民武装警察部队工程	李瑞峰，王绪安，杨海滨，钮可，汤殿华，杨晓元

		auditing of cloud data with designated verifier for batch audit		and Information Sciences		2.07.020	大学	
9	论文	Constant-size ring signature scheme using multilinear maps	中国	International Journal of Embedded Systems	2020-01-01	10.1504/IJES.2020.105930	西安电子科技大学	张襄松，刘振华，王绪安，王凤和
10	论文	Further observation on proxy re-encryption with keyword search	中国	journal of systems and software	2012-08-01	10.1016/j.jss.2011.09.035	中国人民武装警察部队工程大学	王绪安，黄欣沂，杨晓元，刘龙飞，吴旭光

七、主要完成人情况表

姓　　名	杨晓元	排　　名	1
行政职务	无		
技术职称	教授		
工作单位	中国人民武装警察部队工程大学		
完成单位	中国人民武装警察部队工程大学		
对本项目主要学术贡献： 参与对日本 NTT DATA（三菱数据公司）密码学者 Matsuo 提交给 IEEE P1363 标准工作组关于代理重加密的草案进行了密码学分析、建立了发方代理重加密体制的理论体系、构建了 BGV 型多密钥全同态加密方案的密文扩展形式。			

姓　　名	王绪安	排　　名	2
行政职务	无		
技术职称	教授		
工作单位	中国人民武装警察部队工程大学		
完成单位	中国人民武装警察部队工程大学		
对本项目主要学术贡献： 参与对日本 NTT DATA（三菱数据公司）密码学者 Matsuo 提交给 IEEE P1363 标准工作组关于代理重加密的草案进行了密码学分析、建立了发方代理重加密体制的理论体系，参与提出了一种支持批量审计的高效无证书指定审计者云数据完整性审计方案。			

姓　　名	周潭平	排　　名	3
行政职务	无		
技术职称	副教授		
工作单位	中国人民武装警察部队工程大学		
完成单位	中国人民武装警察部队工程大学		

对本项目主要学术贡献： 参与构建了 BGV 型多密钥全同态加密方案的密文扩展形式、提升了 NTRU 型多密钥全同态加密的效率和扩展了参数选择的范围、设计了抗量子的全同态代理重加密方案。

姓　　名	韩益亮	排　　名	4
行政职务	无		
技术职称	教授		
工作单位	中国人民武装警察部队工程大学		
完成单位	中国人民武装警察部队工程大学		
对本项目主要学术贡献： 参与构建了 BGV 型多密钥全同态加密方案的密文扩展形式、提升了 NTRU 型多密钥全同态加密的效率和扩展了参数选择的范围、设计了抗量子的全同态代理重加密方案。			

姓　　名	汤殿华	排　　名	5
行政职务	无		
技术职称	高级工程师、重大任务副总设计师		
工作单位	中国电子科技集团公司第三十研究所		
完成单位	中国电子科技集团公司第三十研究所		
对本项目主要学术贡献： 参与提出了一种支持批量审计的高效无证书指定审计者云数据完整性审计方案。方案使用高效的无证书指定验证者数字签名算法构建方案，利用动态哈希表数据结构对云端数据进行高效地更新。方案能够抵抗不诚实云端的伪造攻击，安全性较高，且与同类型的方案相比，审计效率较高。			

姓　　名	李朋林	排　　名	6
行政职务	上海同态信息科技有限责任公司董事长		
技术职称	无		

工作单位	上海同态信息科技有限责任公司
完成单位	上海同态信息科技有限责任公司
对本项目主要学术贡献： 提出了基于账号隐匿的第三方有效身份托管敏捷认证访问方法。通过搭建第三方身份认证服务平台，以“态安全”APP 为用户操作载体，建立统一的多因素交互身份认证接口并提供给所有公司开放使用，对接入公司进行身份认证服务并将用户认证结果以可证明的形式提供给接入公司的三方有效身份托管敏捷认证访问方法。	

姓　　名	刘振华	排　　名	7
行政职务	无		
技术职称	教授		
工作单位	西安电子科技大学		
完成单位	西安电子科技大学		
对本项目主要学术贡献： 在数据完整性认证方面，使用多线性映射设计了一个具有常数签名长度的环签名方案。在标准模型下，基于多线性计算性 Diffie-Hellman 困难问题假设，该方案被证明抵抗完全密钥泄露是匿名安全的，抵抗选择子环攻击是不可伪造的。进一步地，该方案使用最优安全规约技术具有紧安全规约的优点。			

姓　　名	吴立强	排　　名	8
行政职务	无		
技术职称	讲师		
工作单位	中国人民武装警察部队工程大学		
完成单位	中国人民武装警察部队工程大学		
对本项目主要学术贡献： 参与设计了多个基于格的具有附加性质的代理重加密方案，包括基于格的多跳单向基于身份的代理重加密方案，基于理想格的鲁棒门限代理重加密方案，格上抗合谋攻击的代理重加密方案，全同态代理重加密方案等。			

姓　　名	刘龙飞	排　　名	9

行政职务	无
技术职称	讲师
工作单位	中国人民武装警察部队工程大学
完成单位	中国人民武装警察部队工程大学
对本项目主要学术贡献： 参与构建了 BGV 型多密钥全同态加密方案的密文扩展形式、提升了 NTRU 型多密钥全同态加密的效率和扩展了参数选择的范围、设计了基于格的多跳单向基于身份的代理重加密方案，全同态代理重加密方案等。	

八、主要完成单位情况表

单位名称	中国人民武装警察部队工程大学
对本项目主要学术贡献： 对日本 NTT DATA（三菱数据公司）密码学者 Matsuo 提交给 IEEE P1363 标准工作组关于代理重加密的草案进行了密码学分析、建立了发方代理重加密体制的理论体系、构建了 BGV 型多密钥全同态加密方案的密文扩展形式。	

单位名称	中国电子科技集团公司第三十研究所
对本项目主要学术贡献： 提出了一种支持批量审计的高效无证书指定审计者云数据完整性审计方案。方案使用高效的无证书指定验证者数字签名算法构建方案，利用动态哈希表数据结构对云端数据进行高效地更新。方案能够抵抗不诚实云端的伪造攻击，安全性较高，且与同类型的方案相比，审计效率较高。	

单位名称	西安电子科技大学
对本项目主要学术贡献： 在数据完整性认证方面，使用多线性映射设计了一个具有常数签名长度的环签名方案。在标准模型下，基于多线性计算性 Diffie-Hellman 困难问题假设，该方案被证明抵抗完全密钥泄露是匿名安全的，抵抗选择子环攻击是不可伪造的。进一步地，该方案使用最优安全规约技术具有紧安全规约的优点。	

单位名称	上海同态信息科技有限责任公司
对本项目主要学术贡献： 提出了基于账号隐匿的第三方有效身份托管敏捷认证访问方法 。通过搭建第三方身份认证服务平台，以“态安全”APP 为用户操作载体，建立统一的多因素交互身份认证接口并提供给所有公司开放使用，对接入公司进行身份认证服务并将用户认证结果以可证明的形式提供给接入公司的三方有效身份托管敏捷认证访问方法。	

完成人合作关系说明

中国人民武装警察部队工程大学、中国电子科技集团公司第三十研究所、西安电子科技大学、上海同态信息科技有限责任公司，分工明确、优势互补、联合攻关，对开放环境下数据安全共享与处理关键技术进行了深入研究，合作提出了多项数据安全共享与处理关键技术。

中国人民武装警察部队工程大学杨晓元、王绪安、周潭平、韩益亮、吴立强、刘龙飞系同事关系，长期从事密码学与信息安全相关研究，形成了稳定的科研团队，共同完成了多项国家重点研发计划项目、国家自然科学基金项目、陕西省自然科学基金项目的研究工作。

中国人民武装警察部队工程大学、中国电子科技集团公司第三十研究所自 2009 年开始合作，先后共同合作承担了国家重点研发计划项目“新型数据保护密码算法研究项目”（编号 2017YFB0802000）等项目，在项目内容 2 的支持批量审计的高效无证书指定审计者云数据完整性审计方案中，中国人民武装警察部队工程大学与中国电子科技集团公司第三十研究所有明确合作。

中国人民武装警察部队工程大学、西安电子科技大学自 2000 年开始合作，先后共同合作承担了国家重点研发计划项目“新型数据保护密码算法研究项目”（编号 2017YFB0802000）等项目，在项目内容 2 的具有常数签名长度的环签名方案中，中国人民武装警察部队工程大学与西安电子科技大学有明确合作。

中国人民武装警察部队工程大学、上海同态信息科技有限责任公司、西安电子科技大学自 2019 年开始合作，特别是在开放环境下数据安全处理关键技术中有重要合作。上海同态信息科技有限责任公司、西安电子科技大学在参与编写《云计算中同态加密技术应用要求》团体标准中有着深入的合作。

完成人合作关系情况汇总表

序号	合作方式	合作者/项目排名	合作起始时间	合作完成时间	合作成果	证明材料
1	论文合著	王绪安，汤殿华/2，5	2009 年	至今	Efficient certificateless public integrity auditing of cloud data with designated verifier for batch audit	知识产权 8
2	专利合作	王绪安，杨晓元/2，1	2002 年	至今	组播通信用代理重加密方法	知识产权 1
3	论文合著	王绪安，刘振华/2，7	2017	至今	Constant-size ring signature scheme using multilinear maps	知识产权 9
4	论文合著	吴立强，刘龙飞/8，9	2010	至今	New identity based proxy re-encryption scheme from lattices	知识产权 6
5	专利合作	周潭平，韩益亮/3，4	2012	至今	一种 BGV 型多密钥全同态加密方法	知识产权 2
6	共同参与团体标准制定	李朋林，刘振华/6，7	2020	至今	云计算中同态加密技术应用要求	附件材料