附件

提名项目情况表

<table>
<tr><td colspan="2">项 目 名 称</td><td>面向分布式系统的密码理论研究与应用</td></tr>
<tr><td colspan="2">提 名 等 级</td><td>二等奖</td></tr>
<tr><td colspan="2">主要完成单位</td><td>福建师范大学，武汉大学，中国科学院软件研究所，矩阵元技术（深圳）有限公司</td></tr>
<tr><td colspan="2">主 要 创 新 点</td><td>1. 非交互更新的密钥分散与协同计算技术：借鉴分层密钥派生思想，针对分布式系统的隐私保护与多方协同签署需求，刻画自更新假名/密钥派生的语义和安全模型，设计了首个可提取匿名的分层派生协议，满足分布式场景中非交互密钥更新的应用需求。
2. 多维度可监管的分布式系统隐私保护方法：采取“统筹设计、逐一突破”的布局思路，分别针对身份匿名可查和数据隐私可验两个层面，创新提出“一次一身份+密钥持有证明”的设计方法，实现分布式系统的隐私可监管。
3. 基于密码技术的异步共识性能优化理论：首次在信息扩散协议创新引入密码学证明方法，融合密码技术提出首个“扩散-恢复”两阶段的异步可证明扩散广播协议，解决了20年长期存在的公开问题。</td></tr>
<tr><td colspan="2">主要完成人</td><td rowspan="2">主要完成人贡献</td></tr>
<tr><td>排序</td><td>姓 名</td></tr>
<tr><td>1</td><td>林 超</td><td>1. 实质性贡献：提出可提取匿名的密钥派生方法，并设计了匿名可监管的数据请求协议以及分布式系统的密态可验证的数据隐私保护方案；
2. 关键技术1和2、创新点1和2的贡献者；
3. 在本项目投入的工作量约占本人总工作量90%。</td></tr>
<tr><td>2</td><td>黄欣沂</td><td>1. 实质性贡献：刻画了自更新假名/密钥派生的语义和安全模型，提出了“一次一身份+密钥持有证明”设计方法，实现了匿名认证与规范监管；
2. 关键技术2、创新点2的贡献者；
3. 在本项目投入的工作量约占本人总工作量50%。</td></tr>
<tr><td>3</td><td>路 远</td><td>1. 实质性贡献：基于密码技术设计首个异步可证明扩散广播协议，解决了公开问题，提出多项指标理论最优的异步多值拜占庭共识协议；
2. 关键技术3、创新点3的贡献者；
3. 在本项目投入的工作量约占本人工作量80%。</td></tr>
</table>

4	冯　琦	1. 实质性贡献：针对密钥泄露问题，提出了多方场景下的密钥分散方法，并设计了无需重构密钥的两方协同签名方案，有效降低了密钥泄露风险； 2. 关键技术 1、创新点 1 的贡献者； 3. 在本项目投入的工作量约占本人工作量 70%。
5	龚自洪	1. 实质性贡献：基于密钥保护方案、规范监管机制、高效共识协议进行系统设计与开发，集成各项关键技术并优化性能； 2. 关键技术 1、2 和 3，以及创新点 2 的贡献者； 3. 在本项目投入的工作量约占本人工作量 40%。
6	罗　敏	1. 实质性贡献：针对密态数据可验证需求，设计了高效可批量验证的知识签名方案； 2. 关键技术 2、创新点 2 的贡献者； 3. 在本项目投入的工作量约占本人工作量 30%。
7	何德彪	1. 实质性贡献：提出分布式场景下密钥安全存储和使用方案；在分布式场景下，提出了可证明安全的多方协同签名方案；围绕分布式系统的隐私保护与可监管需求，设计了总体架构和关键组件。 2. 关键技术 1 和 2、创新点 1 和 2 的贡献者； 3. 在本项目投入的工作量约占本人工作量 40%。