

提名项目情况表

项目名称	面向分布式系统的密码理论研究与应
提名等级	二等奖
主要完成单位	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
主要创新点	<p>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，刻画自更新匿名/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。</p> <p>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性和数据隐私可性，提出</p>

主要创新点	<p>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，刻画自更新匿名/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。</p> <p>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性和数据隐私可性，提出</p>
主要创新点	<p>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，刻画自更新匿名/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。</p> <p>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性和数据隐私可性，提出</p>
主要创新点	<p>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，刻画自更新匿名/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。</p> <p>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性和数据隐私可性，提出</p>

4	冯琦	<ol style="list-style-type: none"> 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； 关键技术 1、创新点 1 的贡献者； 在本项目投入的工作量约占本人工作量 70%。
5	龚自洪	<ol style="list-style-type: none"> 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； 关键技术 1、2 和 3，以及创新点 2 的贡献者； 在本项目投入的工作量约占本人工作量 40%。
6	罗敏	<ol style="list-style-type: none"> 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； 关键技术 2、创新点 2 的贡献者； 在本项目投入的工作量约占本人工作量 30%。
7	何德彪	<ol style="list-style-type: none"> 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。 关键技术 1 和 2、创新点 1 和 2 的贡献者； 在本项目投入的工作量约占本人工作量 40%。