学术论文｜我院赛博安全与密码技术团队在区块链方向发表系列成果

发布日期: 2023-06-12, 周一 发布人: 赵胜南

近日，我院赛博安全与密码技术团队的两篇论文分别被**IEEE Transactions on Dependable and Secure Computing**（简称TDSC）和**IEEE Transactions on Information Forensics and Security**（简称TIFS）录用。TDSC和TIFS是中国计算机学会(CCF)推荐的A类期刊，是计算机网络与信息安全研究领域中的顶级期刊。

近年来，我们见证了区块链技术巨大的成功。然而，可扩展性问题使得区块链技术饱受诟病。为缓解该问题，众多学者已经提出了许多不同性质的解决方案。由于其高TPS（每秒交易量），支付通道网络作为最有前途的解决方案而蓬勃发展。**不幸的是，现有的支付通道网络解决方案或者无法提供路径隐私保证，或者需要节点全联通假设**（即，任何两个参与者之间总是存在匿名通信信道）。

赛博安全与密码技术团队首先提出了一种新的密码原语，名为匿名多跳支付（AMHP）。将AMHP与支付通道结合，可以实现一种新的支付通道网络解决方案，该解决方案具有路径隐私属性，但摆脱了节点全联通的假设。随后，该团队提出了第一个AMHP方案，称为AMHL+，但代价是高昂的通信开销。为了降低通信成本，该团队进一步提出了一种基于双线性配对技术的AMHP方案（名为EAMHL+）。与AMHL+相比，EAMHL+的通信成本降低了92.3%。严格的安全分析表明EAMHL+具有一致性、平衡安全性和路径隐私性。最后，大量的实验结果表明，尽管EAMHL+比AMHL+需要更多的计算成本，但就通信开销而言，EAMHL+更加高效。**该匿名多跳支付成果弥补了现有支付通道网络解决方案的不足，为支付通道网络的发展和应用提供了强大动能。**

该成果由浙江工商大学、南京航空航天大学和加拿大新布伦瑞克大学研究人员合作完成，在2023年3月被**IEEE TDSC**录用。**浙江工商大学为该论文的第一完成单位，我院赛博安全与密码技术团队的邵俊教授为论文的通讯作者，硕士三年级研究生张艺同学为该论文的第一作者。**

区块链技术被认为是打破数据孤岛、实现数据流通的有效技术之一，目前已有多个大型区块链项目也相应部署落地。但由于底层区块链系统的异构，导致这些大型区块链项目之间的数据流通十分困难，进而造成新一轮数据孤岛。**针对该问题，工业界和学术界提出了大量跨链协议，但这些协议普遍存在一些弊端，如：单点故障、密钥盗窃、吞吐量低。**

为此，赛博安全与密码技术团队通过研究支付通道和虚拟支付通道，设计了一种新型跨链虚拟支付通道协议。这种协议不仅支持异构链间无速率限制的跨链交易，同时不受中间人状态和底层区块链吞吐量影响，因此可以极大提升跨链交易速率。实验结果证明，研究团队所提协议比已有链下跨链协议更加高效，并且随着跨链交易数量的增加，这种效率优势愈发明显。**该研究成果能够有效优化异构区块链间数据流通，促进区块链技术的发展与应用。**

该成果由浙江工商大学和加拿大新布伦瑞克大学研究人员合作完成，在2023年5月被**IEEE TIFS**录用。**浙江工商大学为该论文的第一完成单位，我院赛博安全与密码技术团队的邵俊教授为论文的通讯作者，硕士二年级研究生贾潇风同学为该论文的第一作者。**

分类: 学院新闻 (/zh-hans/taxonomy/term/56)
科研动态 (/zh-hans/taxonomy/term/29)

专题栏目

› 毕业设计 (http://bysj.zjgsu.edu.cn)
› 实验管理 (http://scielab.zjgsu.edu.cn)
› 学生科技 (http://acm.zjgsu.edu.cn)

平台建设

› 国家及省级平台 (/zh-hans/%E5%B9%B3%E5%8F%B0%E5%BB%BA%E8%AE%BE)

› 软件项目管理平台 (http://zjgsu.5upm.com)

快速链接

› 人才引进 (/zh-hans/%E4%BA%BA%E6%89%8D%E5%BC%95%E8%BF%9B)

› 内部办公 (http://10.21.11.14/cieservice/)

› 办事指南 (/zh-hans/%E5%8A%9E%E4%BA%8B%E6%8C%87%E5%8D%97)

› 文件下载 (/zh-hans/%E6%96%87%E4%BB%B6%E4%B8%8B%E8%BD%BD)

联系方式

地址: 浙江杭州下沙高教园区学正街18号
电话：(86)0571-28008316
邮箱：scie@zjgsu.edu.cn (mailto:scie@zjgsu.edu.cn)

浙公网安备 33011802000512号 (http://www.beian.gov.cn/portal/registerSystemInfo?recordcode=33011802000512)

登录 (/user/login)