计 算 机 学 院

庆祝建校 110 周年系列学术报告

报告题目：面向区块链和金融支付应用的 Gamma-签名及其聚合算法

报 告 人：赵运磊，教授、博导，复旦大学计算机学院

时　　间： 2019.5.28 上午 11:00

地　　点：计算机楼 B518

个人简介：

赵运磊，复旦大学计算机科学技术学院特聘教授(Distinguished Professor)、博导，目前担任中国密码学会理事、信息保障国家重点实验室学术委员会委员等，研究领域为：密码学理论及应用、计算理论和随机计算。在《Journal of Cryptology》、ACMCCS、

EUROCRYPT 等期刊和会议发表多篇论文，研究获得国家973、自然科学基金、国家密码发展基金的支持。多项研究成果得到大规模应用。

报告摘要：聚合签名可以将多个签名以非交互的方式进行聚合，这对区块链提升吞吐率、节省存储空间、提升交易验证效率具有重要意义。已知的聚合签名均基于双线性配对，基于一般椭圆曲线的聚合签名是长期未解决的公开问题。我们提出了一种新的将诚实验证者零知识转换为数字签名的新方法,称为 Gamma-转换。基于 Gamma-转换，我们得到了将 EC-Schnorr 签名和 EC-DSA 签名优点都继承而缺点都避免的新型签名方案，称为 Gamma-签名。我们进一步证明 Gamma-签名支持聚合操作,这是目前已知的唯一的基于一般椭圆曲线的可聚合数字签名方案。在此过程中，我们也通过具体的攻击，表明目前存在的其它一般椭圆曲线数字签名方案无法支持签名聚合。。

欢迎广大师生参加！