北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
前沿讲座

Efficient Threshold ECDSA and Their Applications

Prof. Man Ho Au

Department of Computing
Hong Kong Polytechnic University

Host: 邓小铁 讲席教授
2023年9月23日 星期六 19:00
静园五院204室

Abstract

Elliptic Curve Digital Signature Algorithm (ECDSA) is one of the most popular digital signature scheme deployed in practice. They are widely used in ensuring the authenticity and integrity of messages in various applications. In this talk, we go into the details of distributed ECDSA, exploring its significance, mechanisms, and applications.

The speaker will begin by giving an overview of traditional ECDSA and its role in establishing digital signatures. With growing popularity of the use of ECDSA in blockchains, there is an increasing need to secure the signing key. This talk will delve into the challenges posed by distributed environments, and how Distributed ECDSA rises to address these challenges.

We will formalise the concept of threshold signatures and how they enable multiple parties to collaboratively create a signature without compromising security. Then, we will discuss common approaches to design threshold ECDSA. Finally, we will also discuss how these techniques can be used to support other threshold signatures.

Biography

Prof. Man Ho Au is a Full Professor at the Department of Computing of The Hong Kong Polytechnic University. Before that, he was an Associate Professor in the Department of Computer Science at the University of Hong Kong. His research interests include information security, cryptography, blockchain technology, and their applications. He has published over 200 refereed papers in top journals and conferences, including CRYPTO, ASIACRYPT, ACM CCS, NDSS, IEEE S&P, SIGMOD, SOSP, IEEE TIFS, IEEE TDSC, and others. He is a recipient of the 2009 PET runner-up award for outstanding research in privacy-enhancing technologies. His team won the ZPrize - Open Division Plonk-DIZK GPU Acceleration prize, which came with a cash award of 550K USD. He has served as a program committee/general chair of several international conferences, including ACM ASIACCS, RAID, SECURECOM, ISPEC, PROVSEC, among others. Currently, he is an associate editor of IEEE Transactions on Dependable and Secure Computing, Journal of Information Security and Applications, and an editorial board member of the Journal of Cryptologic Research.

http: //cfcs.pku.edu.cn/