基于秘密共享的安全多方计算简介

Kurt Pan

2023 年 6 月 9 日

目录

目录

引言

A big part of the theory and practice of cryptography is devoted to the study of different technologies deployed in our world today. Standard topics include the task of encryption, which relates to hiding information, but it is also common to consider digital signatures and message authentication codes to ensure integrity, enable authentication and authorization, and many other subjects relevant for today's infrastructure. For centuries, these were essentially the main tasks associated with the idea of securing information and communi- cation, and this continues being the case today—of course, with the added complications of digital and worldwide-distributed technologies. Research into correct implementations and deployments of these tools, possible attacks, improvements, enhancements in user experience, adaptation to modern more technologies and scenarios, and other relevant questions, is of high importance.

目录

第一部分

安全多方计算基础

第 1 章

安全多方计算的理论

1.1 安全多方计算概述

第 2 章

基于秘密共享的安全多方计算

第二部分

诚实多数

第 3 章

Shamir 秘密共享

3.1 秘密共享和 d-一致性

第 4 章

诚实多数被动完美安全

第 5 章

三分之二诚实多数主动完美安全

第 6 章

诚实多数主动统计安全

第三部分

不诚实多数

第 7 章

不诚实多数被动安全

第 8 章

不诚实多数主动安全