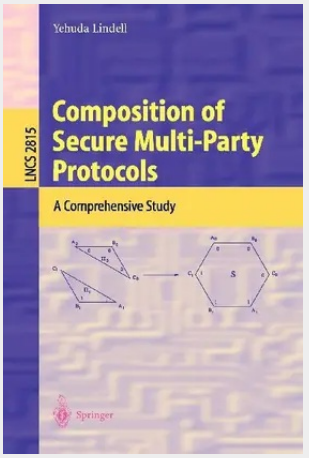
Lindell

Composition of Secure Multi-Party Protocols

A Comprehensive Study



In the setting of multi-party computation, sets of two or more parties with private inputs wish to jointly compute some (predetermined) function of their inputs. General results concerning secure two-party or multi-party computation were first announced in the 1980s. Put briefly, these results assert that under certain assumptions one can construct protocols for securely computing any desired multi-party functionality. However, this research relates only to a setting where a single protocol execution is carried out. In contrast, in modern networks, many different protocol executions are run at the same time.

This book is devoted to the general and systematic study of secure multi-party computation under composition. Despite its emphasis on a theoretically well-founded treatment of the subject, general techniques for designing secure protocols are developed that may even result in schemes or modules to be incorporated in practical systems. The book clarifies fundamental issues regarding security in a multi-execution environment and gives a comprehensive and unique treatment of the composition of secure multi-party protocols.

In the setting of multi-party computation, sets of two or more parties with private inputs wish to jointly compute some (predetermined) function of their inputs. General results concerning secure two-party or multi-party computation were first announced in the 1980s. Put briefly, these results assert that under certain assumptions one can construct protocols for securely computing any desired multi-party functionality. However, this research relates only to a setting where a single protocol execution is carried out. In contrast, in modern networks, many different protocol executions are run at the same time.This book is devoted to the general and systematic study of secure multi-party computation under composition. Despite its emphasis on a theoretically well-founded treatment of the subject, general techniques for designing secure protocols are developed that may even result in schemes or modules to be incorporated in practical systems. The book clarifies fundamental issues regarding security in a multi-execution environment and gives a comprehensive and unique treatment of the composition of secure multi-party protocols.

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540201052
Medium: Buch
ISBN: 978-3-540-20105-2
Verlag: Springer
Erscheinungstermin: 08.09.2003
Sprache(n): Englisch
Auflage: 2003
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 335 g
Seiten: 200
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)