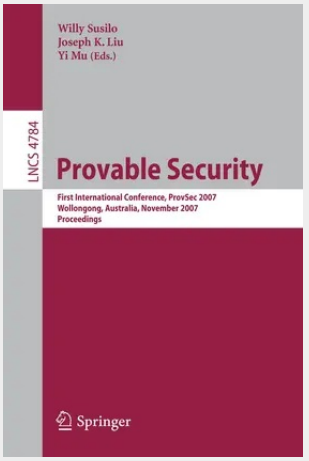
Susilo / Liu / Mu

Provable Security

First International Conference, ProvSec 2007, Wollongong, Australia, November 1-2, 2007. Proceedings



This book constitutes the refereed proceedings of the First International Conference on Provable Security, ProvSec 2007, held in Wollongong, Australia. The 10 revised full papers presented together with seven short papers were carefully reviewed and selected. The papers are organized in topical sections on Authentication, Asymmetric Encryption, Signature, Protocol and Proving Technique, Authentication and Symmetric Encryption, Signature and Asymmetric Encryption.

The First International Conference on Provable Security 2007 (ProvSec 2007) was held in Wollongong, Australia, November 1–2, 2007. The conference was sponsored by iCORE Information Security Laboratory and RNSA (Research Network for a Secure Australia). We are grateful to these organizationsfor their support of the conference. The conference proceedings, representing both full papers and short papers, were published in time for the conference in this volume of Lecture Notes in Computer Science series by Springer. This year the program committee invited an international keynote speaker: Colin Boyd from Queensland University of Technology, Australia. Prof. Boyd's talk addressed the topic of "On One-Pass Key Establishment". The Program Committee received 51 submissions. Ten submissions were - lected for full paper presentation and seven were selected for short paper p- sentation. The reviewing process was run using the iChair software, written by Thomas Baign` eres and Matthieu Finiasz (EPFL, Switzerland). It took seven weeks; each paper was carefully evaluated by at least three members of the P- gram Committee. We appreciate the hard work of the members of the Program Committee and the external referees, who gave many hours of their valuable time. We would like to thank all the people involved in organizing this conference. In particular we would like to thank the General Chair Yi Mu, the Organizing Committee Man Ho Au and Xinyi Huang and the Webmaster, Lan Zhou, for their time and e?orts.

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540756699
Medium: Buch
ISBN: 978-3-540-75669-9
Verlag: Springer
Erscheinungstermin: 24.10.2007
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2007
Serie: Security and Cryptology
Produktform: Kartoniert
Gewicht: 397 g
Seiten: 246
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)