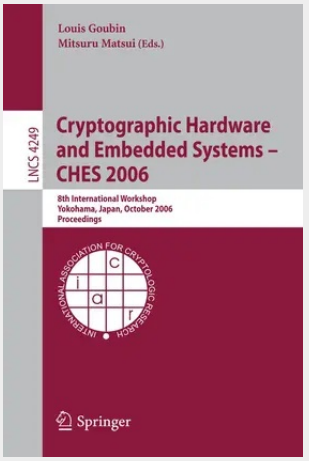
Goubin / Matsui

Cryptographic Hardware and Embedded Systems - CHES 2006

8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings



These are the proceedings of the Eighth Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006) held in Yokohama, Japan, October 10-13, 2006. The CHES workshophas been sponsored by the International Association for Cryptographic Research (IACR) since 2004. The ?rst and the second CHES workshops were held in Worcester in 1999 and 2000, respectively, followed by Paris in 2001, San Francisco Bay Area in 2002, Cologne in 2003, Boston in 2004 and Edinburgh in 2005. This is the ?rst CHES workshop held in Asia. This year,a totalof 112 paper submissionswerereceived.The reviewprocess was therefore a delicate and challenging task for the Program Committee m- bers. Each paper was carefully read by at least three reviewers, and submissions with a Program Committee member as a (co-)author by at least ?ve reviewers. The review process concluded with a two week Web discussion process which resulted in 32 papers being selected for presentation. Unfortunately, there were a number of good papers that could not be included in the program due to a lack of space. We would like to thank all the authors who submitted papers to CHES 2006. In addition to regular presentations, we were very fortunate to have in the programthreeexcellentinvitedtalksgivenbyKazumaroAoki(NTT)on“Integer Factoring Utilizing PC Cluster,” Ari Juels (RSA Labs) on “The Outer Limits of RFID Security” and Ahmad Sadeghi (Ruhr University Bochum) on “Challenges for Trusted Computing.” The program also included a rump session, chaired by Christof Paar, featuring informal presentations on recent results.

These are the proceedings of the Eighth Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006) held in Yokohama, Japan, October 10-13, 2006. The CHES workshophas been sponsored by the International Association for Cryptographic Research (IACR) since 2004. The ?rst and the second CHES workshops were held in Worcester in 1999 and 2000, respectively, followed by Paris in 2001, San Francisco Bay Area in 2002, Cologne in 2003, Boston in 2004 and Edinburgh in 2005. This is the ?rst CHES workshop held in Asia. This year,a totalof 112 paper submissionswerereceived.The reviewprocess was therefore a delicate and challenging task for the Program Committee m- bers. Each paper was carefully read by at least three reviewers, and submissions with a Program Committee member as a (co-)author by at least ?ve reviewers. The review process concluded with a two week Web discussion process which resulted in 32 papers being selected for presentation. Unfortunately, there were a number of good papers that could not be included in the program due to a lack of space. We would like to thank all the authors who submitted papers to CHES 2006. In addition to regular presentations, we were very fortunate to have in the programthreeexcellentinvitedtalksgivenbyKazumaroAoki(NTT)on“Integer Factoring Utilizing PC Cluster,” Ari Juels (RSA Labs) on “The Outer Limits of RFID Security” and Ahmad Sadeghi (Ruhr University Bochum) on “Challenges for Trusted Computing.” The program also included a rump session, chaired by Christof Paar, featuring informal presentations on recent results.

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540465591
Medium: Buch
ISBN: 978-3-540-46559-1
Verlag: Springer
Erscheinungstermin: 27.09.2006
Sprache(n): Englisch
Auflage: 1. Auflage 2006
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 753 g
Seiten: 462
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)