



Cetin K. Koc, David Naccache, Christof Paar (Eds.)

Cryptographic Hardware and Embedded Systems - CHES 2001

Third International Workshop, Paris, France, May 14-16, 2001
Proceedings

Series: Lecture Notes in Computer Science

2001, XIV, 418 p.

Printed book

Softcover

94,99 € | £84.99 | \$119.99
[1]101,64 € (D) | 104,49 € (A) | CHF
112,00

eBook

80,24 € | £67.99 | \$89.00
[2]80,24 € (D) | 80,24 € (A) | CHF
89,50

Available from your library or
springer.com/shop

MyCopy [3]

Printed eBook for just

€ | \$ 24.99

springer.com/mycopy

[Error\[en_EN | Export.Bookseller. MediumType | SE\]](#)

£24.99 | \$24.99

CHF 24,99

These are the proceedings of CHES 2001, the third Workshop on Cryptographic Hardware and Embedded Systems. The first two CHES Workshops were held in Massachusetts, and this was the first Workshop to be held in Europe. There was a large number of submissions this year, and in response the technical program was extended to 2 1/2 days. As is evident by the papers in these proceedings, many excellent submissions were made. Selecting the papers for this year's CHES was not an easy task, and were regrettable that we had to reject several very interesting papers due to the lack of time. There were 66 submitted contributions this year, of which 31, or 47%, were selected for presentation. If we look at the number of submitted papers at CHES '99 (42 papers) and CHES 2001 (51 papers), we observe a steady increase. We interpret this as a continuing need for a workshop series which combines theory and practice for integrating strong security features into modern communications and computer applications. In addition to the submitted contributions, Ross Anderson from Cambridge University, UK, and Adi Shamir from The Weizmann Institute, Israel, gave invited talks. As in previous years, the focus of the workshop is on all aspects of cryptographic hardware and embedded system design. Of special interest were contributions that describe new methods for efficient hardware implementations and high-speed software for embedded systems, e.g., smart cards, microprocessors, DSPs, etc. CHES also continues to be an important forum for new theoretical and practical findings in the important and growing field of side-channel attacks.

Order online at springer.com / or for the Americas call (toll free) 1-800-SPRINGER / or email us at: customerservice@springernature.com. / For outside the Americas call +49 (0) 6221-345-4301 / or email us at: customerservice@springernature.com.

The first € price and the £ and \$ price are net prices, subject to local VAT. Prices indicated with [1] include VAT for books; the €(D) includes 7% for Germany, the €(A) includes 10% for Austria. Prices indicated with [2] include VAT for electronic products; 19% for Germany, 20% for Austria. All prices exclusive of carriage charges. Prices and other details are subject to change without notice. All errors and omissions excepted. [3] No discount for MyCopy.

