Preface

This Fast Software Encryption workshop was the ninth in a series of workshops started in Cambridge in December 1993. The previous workshop took place in Yokohama in April 2001. It concentrated on all aspects of fast primitives for symmetric cryptography: secret key ciphers, the design and cryptanalysis of block and stream ciphers, as well as hash functions and message authentication codes (MACs).

The ninth Fast Software Encryption workshop was held in February 2002 in Leuven, Belgium and was organized by General Chair Matt Landrock (Cryptomathic Belgium), in cooperation with the research group COSIC of K.U. Leuven. This year there were 70 submissions, of which 21 were selected for presentation and publication in this volume.

We would like to thank the following people. First of all the submitting authors and the program committee for their work. Then Markku-Juhani O. Saarinen, Orr Dunkelman, Fredrik Jönsson, Helger Lipmaa, Greg Rose, Alex Biryukov, and Christophe De Canniere, who provided reviews at the request of program committee members. Bart Preneel for letting us use COSIC's Web-review software in the review process and Wim Moreau for all his support. Finally we would like to thank Krista Geens of Cryptomathic for her help in the registration and the practical organization.

May 2002 Joan Daemen and Vincent Rijmen

Fast Software Encryption 2002

February 4–6, 2002, Leuven, Belgium

Sponsored by the
International Association for Cryptologic Research

General Chair

Matt Landrock, Cryptomathic, Belgium

Program Co-chairs

Joan Daemen, Proton World, Belgium
Vincent Rijmen, Cryptomathic, Belgium

Program Committee

Ross Anderson ..... Cambridge University, UK
Eli Biham ..... Technion, IL
Don Coppersmith ..... IBM, USA
Cunshen Ding ..... Hong Kong University of Science and Technology, HK
Thomas Johansson ..... Lund University, SE
Mitsuru Matsui ..... Mitsubishi Electric, JP
Willi Meier ..... Fachhochschule Aargau, CH
Kaisa Nyberg ..... Nokia, FI
Bart Preneel ..... Katholieke Universiteit Leuven, BE