Preface

Fast Software Encryption is an eight-year-old workshop on symmetric cryptography, including the design and cryptanalysis of block and stream ciphers, as well as hash functions. The first Fast Software Encryption Workshop was held in Cambridge in 1993, followed by Leuven in 1994, Cambridge in 1996, Haifa in 1997, Paris in 1998, Rome in 1999, and New York in 2000. This Fast Software Encryption Workshop, FSE 2001, was held from 2-4 April 2001 in Yokohama, Japan, in cooperation with the Institute of Industrial Science, of the University of Tokyo.

This year a total of 46 papers were submitted to FSE 2001. After a two-month review process, 27 papers were accepted for presentation at the workshop. In addition, we were fortunate to be able to organize a special talk by Bart Preneel on the NESSIE project, a European initiative to evaluate cryptographic algorithms. The committee of this workshop was:

General Chair
Hideki Imai (The University of Tokyo)

Program Committee

Ross Anderson (Cambridge Univ.)	Eli Biham (Technion)
Cunsheng Ding (Singapore)	Henri Gilbert (France Telecom)
Dieter Gollman (Microsoft)	Thomas Johansson (Lund Univ.)
Lars Knudsen (Bergen Univ.)	James Massey (Denmark)
Mitsuru Matsui (Mitsubishi Electric, Chair)	Kaisa Nyberg (Nokia)
Bart Preneel (Katholieke Univ. Leuven)	Bruce Schneier (Counterpane)

We would like to thank all submitting authors and the committee members for their hard work. We are also appreciative of the financial support provided by Mitsubishi Electric Corporation. Special thanks are due to Toshio Tokita, Junko Nakajima, Yasuyuki Sakai, Seiichi Amada, Toshio Hasegawa, Katsuyuki Takashima, and Toru Sorimachi for their efforts in making the local arrangements for this workshop.

We were very pleased and honored to host the first FSE workshop held in Asia. Finally, we are also happy to announce that the next FSE will be the first FSE workshop sponsored by International Association for Cryptologic Research (IACR).

May 2002 Mitsuru Matsui